Addendum 1

Updated_Addendum 1
DATED [01-10-2026]

FOR

SELECTION OF BIDDER FOR SUPPLY INSTALLATION, IMPLEMENTATION, MAINTENANCE & MANAGEMENT OF NEXTGEN SOC & RELATED SERVICES

BID NO: PSB/ HO-CISO CELL/2026-27/RFP_01 DATED 09/09/2026
GEM BID No. GEM/2026/B/8018719 dated 09/09/2026

Punjab & Sind Bank
Staff Training Centre
CISO Cell, 3rd Floor
B-8/232, Naharpur Village Road, Pocket 8, Sector 3B,
Rohini, Delhi, 110085

This document is the property of Punjab and Sind Bank. It may not be copied, distributed or recorded on any medium, electronic or otherwise, without written permission thereof. The use of the contents of this document, even by the authorized personnel/agencies for any purpose other than the purpose specified herein, is strictly prohibited and shall amount to copyright violation and thus, shall be punishable under the Indian Law.

Please consider this version_ references has been corrected

Section of the Document	Page No.
Addendum 1	2
Updated RFP based on Addendum	42
Appendix 1A	342
Appendix 1B	403
Appendix 1C	419
Appendix 2 – Commercial BOM	438
Pre- Bid Queries Reply	459

Note: The Bank will allow only one clarification opportunity, Evaluation will be based solely on documents and evidence submitted with the bid. No new credentials will be accepted subject to Bank's Discretion. Furthermore, All Bidder's personnel deployed on the project shall be on the Bidder's payroll. The Bidder shall submit the relevant EPFO and ESIC details/documents of each of the personnel to the Bank for verification of their employment status.

Addendum 1
DATED [30-09-2026]

FOR

SELECTION OF BIDDER FOR SUPPLY INSTALLATION, IMPLEMENTATION, MAINTENANCE & MANAGEMENT OF NEXTGEN SOC & RELATED SERVICES

BID NO: PSB/ HO-CISO CELL/2026-27/RFP_01 DATED 09/09/2026
GEM BID No. GEM/2026/B/8018719 dated 09/09/2026

Punjab & Sind Bank
Staff Training Centre
CISO Cell, 3rd Floor
B-8/232, Naharpur Village Road, Pocket 8, Sector 3B,
Rohini, Delhi, 110085

This document is the property of Punjab and Sind Bank. It may not be copied, distributed or recorded on any medium, electronic or otherwise, without written permission thereof. The use of the contents of this document, even by the authorized personnel/agencies for any purpose other than the purpose specified herein, is strictly prohibited and shall amount to copyright violation and thus, shall be punishable under the Indian Law.

Addendum 1

Introduction

Bank has published the RFP vide tender No: BID NO: PSB/ HO-CISO CELL/2026-27/RFP_01 dated 09/09/2026 (GeM Bid No. GEM/2026/B/8018719) for SELECTION OF BIDDER FOR SUPPLY INSTALLATION, IMPLEMENTATION, MAINTENANCE & MANAGEMENT OF NEXTGEN SOC & RELATED SERVICES.

Following amendments have been made in the above stated RFP. All other terms and conditions of the RFP shall remain unchanged. Please treat this Addendum as an integral part of the RFP documents issued.

With reference to the aforesaid RFP, all are advised to note following:

Section 1: Modification in RFP Dates:

S.No.	Pg No.	RFP Section	Original Date	Revised Date
1.	**RFP Page No. 8**	**Key Information:** Last Date and Time for submission of Bids	As per GeM Portal (Bid End Date/Time: 12-10-2026, 3:00 PM)	As per GeM Portal
2.	**RFP Page No. 8**	**Key Information:** Date and Time of Opening of Bids	As per GeM Portal (Bid Opening Date/Time: 13-10-2026, 3:00 PM)	As per GeM Portal

Addendum 1

Section 2: Updated RFP

The attached updated RFP document shall be considered for bid preparation and submission and further referencing.

Also, bidders can download the updated Excel file from the bank's website for their reference.

Section 3: Modification in RFP Clauses:

#	Pre Bid/RFP Reference	Page No.	Published RFP Clause	Updated Clause	Revised RFP Reference
RFP					
1.	Section 7.1	26	New Point	Key Architecture points to be followed: • All solutions, products, platforms, technologies, and services proposed by the Bidder under this RFP shall be AI-enabled and shall leverage Artificial Intelligence (AI), automation, advanced analytics, or intelligent orchestration to enhance service delivery, operational efficiency, security, automation, and continuous improvement. • All proposed solutions and services, wherever applicable, shall integrate with the Bank's Security Information and Event Management (SIEM) platform. • The Bank's architecture requires that all communication/traffic shall traverse through the Bank's designated infrastructure/security controls, unless explicitly approved otherwise by the Bank. • All SaaS-based proposed solutions shall be designed such that all logs, data, information, scan results, credentials-related metadata, and other security information collected from the Bank's on-	Refer Section 7.1 – Scope and Objective

Addendum 1

#	Pre Bid/RFP Reference	Page No.	Published RFP Clause	Updated Clause	Revised RFP Reference
RFP					
				premises infrastructure are first collected and processed by the on-premises scanning component. The on-premises component shall then securely transmit only the required data to the SaaS platform over encrypted communication channels. • Should have dedicated logical tenant provisioned for bank. • Customer PII shall not be stored, processed, or transmitted through cloud infrastructure. • The proposed solution fully secure through Bank-controlled BYOK encryption and exclusive PSB admin authority. • The proposed solution shall support PQC readiness, including support for secure cryptographic mechanisms and standards that facilitate future migration to quantum-resistant cryptography, wherever applicable to the solution. The bidder shall provide the required SSL/TLS certificate for securing data in motion throughout the contract period at no additional cost to the bank. • All the proposed solution	

Addendum 1

#	Pre Bid/RFP Reference	Page No.	Published RFP Clause	Updated Clause	Revised RFP Reference
RFP					
				○ are the latest commercially available and supported Model(s) and Version(s) offered by the OEM for the relevant product category as on the date of submission of the Bid; ○ are not declared End-of-Sale (EoS) as on the date of submission of the Bid; and ○ shall remain supported by the OEM and shall not reach End-of-Life (EoL) / End-of-Support (EoS) during the Contract Period or for a period of six (6) years from the date of product installation, whichever is later • OEM architecture should have aggregation at bank's DC & DR through agents/ collectors/ brokers/ aggregators, sensors/ connectors/ scanners, enforcers/ integrators or equivalent components. The SaaS service shall comply with the uptime SLA and other service availability requirements specified in this RFP • The proposed architecture shall therefore be designed to comply with this requirement	

Addendum 1

#	Pre Bid/RFP Reference	Page No.	Published RFP Clause	Updated Clause	Revised RFP Reference
RFP					
2.	Section 6.4.1.1 Masked Bill of Material (BoM) – Technical Proposal	17	A Masked Bill of Material (BoM) must be submitted as part of the Technical Proposal and shall not contain any commercial or pricing information whatsoever. (Followed by four paragraphs on the coverage, format and non-compliance of the Masked BoM.)	The Masked BoM requirements have been moved to Annexure 1: Submission Checklist, under 'Filling Notes: Masked Bill of Material'. All commercial information, including unit cost, total cost, taxes, GST, discounts, duties and any other commercial value, shall be masked as "XX".	Refer Section 16.1 – Annexure 1: Submission Checklist (Filling Notes: Masked Bill of Material)
3.	Section 6.10 Earnest Money Deposit (EMD), Point 2	20	New point.	The Bidder may also submit the EMD in the form of an Insurance Surety Bond. Refer Annexure 34: Insurance Surety Bond	Section 16.35 – Annexure 34: Insurance Surety Bond against EMD
4.	Section 7.1 Scope and Objectives	26-27	Key Implementation Responsibilities Key Roles and Responsibilities:	a. Key Implementation Responsibilities, but not limited to: b. Key Roles and Responsibilities, but not limited to: f. New: The proposed solutions shall provide configurable dashboards, analytics, executive reports, operational reports, compliance reports, and actionable insights for effective monitoring, governance, and decision-making. Please refer Annexure 25: Indicative List of Reports to be Provided.	Refer Section 7.1 – Scope and Objectives and Section 16.26 – Annexure 25
5.			New Section	Added RACI Matric	Refer Section 7.1.1 RACI Matrix
6.	Section 7.2 Solution & Services Deployment	29-32	Section 7.2.1 Solutions – Master Deployment Matrix Section 7.2.2 Services	Please refer Annexure 21	Please refer Annexure 21

Addendum 1

#	Pre Bid/RFP Reference	Page No.	Published RFP Clause	Updated Clause	Revised RFP Reference
RFP					
	Model and Their HA Requirement		Section 7.2.3 Deployment Model Definition Section 7.2.4 Deployment Architecture		
7.	Section 7.3.9.1 Modules, Architecture & Deployment (ITDR), Point 3	48	The solution shall support integration with relevant identity sources, including Active Directory, LDAP, IAM, PAM, SSO, cloud identity providers and other Bank-approved identity repositories, as applicable.	The solution shall support integration with relevant identity sources, including Active Directory, Entra ID, LDAP, IAM, SSO, cloud identity providers and other Bank-approved identity repositories, as applicable.	Refer Section 7.3.9.1, Point 3
8.	Section 7.3.11.2 Key Deliverables (CSPM), Point 12	51	Ensure that the reports are extracted from online / warehouse storage etc. Restore the logs/data from backup for forensic investigation and as per bank requirement without any additional cost.	Clause stands deleted.	Refer Section 7.3.11.2 – Key Deliverables (CSPM) (Point 12 of the published RFP deleted)
9.	Section 7.3.14 Continuous Threat Exposure Management (CTEM) Tool, Paragraph 2	53	The Bidder shall leverage all the required services and technologies to provide an integrated, unified 'Risk Dashboard' that operationalizes the 5 stages of the CTEM framework (Scoping, Discovery, Prioritization, Validation, and Mobilization). This dashboard must provide a single-pane-of-glass view that correlates technical vulnerabilities (VM) with simulated attack paths (BAS), allowing the Bank to visualize the real-world exploitability of its critical assets.	The Bidder shall leverage all the required services and technologies to provide an integrated, unified 'Risk Dashboard' that operationalizes the 5 stages of the CTEM framework (Scoping, Discovery, Prioritization, Validation, and Mobilization). This dashboard must provide a single-pane-of-glass view that correlates technical vulnerabilities (VM) with simulated attack paths (BAS), allowing the Bank to visualize the real-world exploitability of its assets.	Refer Section 7.3.14, Paragraph 2
10.	Section 7.3.14.1 Modules, Architecture &	53	The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's	The proposed solution should have Two-Factor Authentication (2FA) and as an when bank brings it's own MFA then solution should also be capable of integrating with	Refer Section 7.3.14.1, Point 2

Addendum 1

#	Pre Bid/RFP Reference	Page No.	Published RFP Clause	Updated Clause	Revised RFP Reference
RFP					
	Deployment (CTEM), Point 2		existing Multi-Factor Authentication (MFA) solution.	the bank's existing Multi-Factor Authentication (MFA) solution.	
11.	Section 7.4.3 Attack surface management – service inclusions (bullets 1 and 2) and introductory paragraph	56	The Bidder shall provide continuous discovery, monitoring, classification, and risk assessment of the Bank's external and internal attack surface. • Discovery of internet-facing and internal assets. • Identification of exposed services, applications, APIs, domains, cloud assets, certificates, and digital infrastructure.	The Bidder shall provide continuous discovery, monitoring, classification, and risk assessment of the Bank's internet-facing & external surface. • Discovery of internet-facing & external assets. • Identification of exposed services, applications, domains, cloud assets, certificates, and digital infrastructure.	Refer Section 7.4.3 – Attack Surface Management
12.	Section 7.3.5 NDR	56	Entire Section 7.3.5 NDR	The Network Detection and Response (NDR) requirement has been deleted. Accordingly, the corresponding capabilities should be demonstrated through the proposed XDR platform, refer revised XDR specification.	Refer Section 7.3.5 – NDR & Refer Section 7.3.4 – XDR
13.	Section 7.4.5 Anti-Phishing	56	Entire Section 7.4.5 Anti-Phishing	This clause stands deleted. The Anti-Phishing services have been moved under the Digital Risk Management scope	Refer Section 7.4.5 – Anti-Phishing
14.	Section 7.4.9- Brand Protection and Monitoring	58	Entire Section 7.4.9 Brand Protection and Monitoring (Brand Abuse)	This clause stands deleted. The Brand Abuse services have been moved under the Digital Risk Management scope	Section 7.4.9- Brand Protection and Monitoring (Brand Abuse)
15.	Section 7.6.5 Deployment and Go-Live - Activities are to be performed by		New Point	The Bidder and respective OEM shall deploy & implement bank's identified existing security rules, policies, use cases, configuration, and other learnings from bank's existing technologies/solutions.	Refer Section 7.6.5 - Deployment and Go-Live - Activities are to be performed by Respective Solution OEM (supported by bidder)

Addendum 1

#	Pre Bid/RFP Reference	Page No.	Published RFP Clause	Updated Clause	Revised RFP Reference
RFP					
	Respective Solution OEM				(Point 2)
16.	Section 7.6.6 Testing, Point 3	64	The bidder shall provision and maintain dedicated Development, Testing, UAT, and Pre-Production environments throughout the contract period. All software, licenses, and other resources required for such environments shall be included within the bidder's scope without any additional cost to the Bank.	Clause stands deleted	Refer Section 7.6.6 – Testing (Point 3 of the published RFP deleted; subsequent points renumbered)
17.	7.6.7 Training- Activities are to be performed by Respective solution OEM	66	Entire Section 7.6.7 Training- Activities are to be performed by Respective solution OEM (supported by bidder)	Please refer Section 7.6.7 for the revised requirements of Training	7.6.7 Training- Activities are to be performed by Respective solution OEM (supported by bidder)
18.	Section 7.7 On-cloud proposed solution OEM Responsibilities, Point 1	68	The security telemetry received by the OEM Cloud platform will be routed to the dedicated tenant/workspace provisioned for the Bank.	The security telemetry received by the OEM Cloud platform will be routed to the dedicated logical tenant/workspace provisioned for the Bank.	Refer Section 7.7, Point 1
19.	Section 7.7 On-cloud proposed solution OEM Responsibilities, Point 8	68	The solution shall support secure connectivity with the Bank's on-premises infrastructure, cloud environments, and external systems through private and secure communication mechanisms.	The solution shall support secure connectivity with the Bank's on-premises infrastructure, cloud environments, and external systems through private or secure communication mechanisms via internet, or the tenant can be restricted based on Bank's static public IP addresses.	Refer Section 7.7, Point 8

Addendum 1

#	Pre Bid/RFP Reference	Page No.	Published RFP Clause	Updated Clause	Revised RFP Reference
RFP					
20.	Section 7.12 Resource Requirements	73-74	Section 7.12.2 and 7.12.3	Refer Section 7.12 of Resource Requirement for updated Qualification	Refer Section 7.12 – Resource Requirement
21.	Section 7.18 IT Infrastructure requirements, Point 3	89	The proposed hardware infrastructure should be of the latest production available infrastructure not older than 2025.	The proposed IT Infrastructure/Hardware Appliances model should not be end of sale product at the time of bid submission, and supportability (End of Life or End of support) of the product should be available for the entire contract period. Bidder to submit the undertaking on OEM's letterhead as per Annexure 26: Undertaking – Support & Launch Confirmation.	Refer Section 7.18, Point 3
22.	Section 7.18 IT Infrastructure requirements, Point 9 (Non-production)	89	Bidder has to propose a dedicated non-production environment which can logically separate / Virtualized for Test, Development and Training. For all component/solution proposed on-premises, the bidder should note that the production and non-production environment should be physically separate to meet the requirement of the PSB.	Clause stands deleted.	Refer Section 7.18 – IT Infrastructure requirements (Point 9 of the published RFP deleted)
23.	Section 7.18 IT Infrastructure requirements, Point 21	91	Non-Production Environment: a) The non-production environment must be physically/logically separated from the production environment.	Clause stands deleted.	Refer Section 7.18 – IT Infrastructure requirements (Point 21 of the published RFP deleted; subsequent points renumbered)
24.	Section 7.18.1 Compute	91	The production and non-production environment should be physically separated to meet the requirement of the bank.	The production and non-production environment should be separated to meet the requirement of the bank.	Refer Section 7.18.1, Point 8

Addendum 1

#	Pre Bid/RFP Reference	Page No.	Published RFP Clause	Updated Clause	Revised RFP Reference
RFP					
	Infrastructure, Point 8				
25.	Section 7.18.1 Compute Infrastructure, Point 10	92	Non-production: a) The non-production environments should have the same software and hardware setup as deployed in production environments meeting all RFP requirements.	Clause stands deleted.	Refer Section 7.18.1 – Compute Infrastructure (Point 10 of the published RFP deleted; subsequent points renumbered)
26.	Section 8 Contract Period	98	The contract period for the project is the Implementation Period (as mentioned in Section 9: Project Timelines) + Support period (60 Month Post Go-live) which will commence from the effective date of agreement.	The contract period for the project is the Implementation Period (as mentioned in Section 9: Project Timelines) + Support period (60 Month Post Go-live) which will commence from the date of acceptance of PO. Effective start date for the contract would be date of acceptance of the PO.	Refer Section 8 – Contract Period
27.	Section 10.1 Preliminary Scrutiny		Bidders are therefore advised to ensure that all required documents and supporting evidence are submitted along with the bid. The Bank shall evaluate the bid based on the documents originally submitted and any permissible clarifications sought by the Bank. The Bank's decision regarding the adequacy, relevance, interpretation, compliance, and evaluation of the submitted documents and information shall be final, conclusive, and binding on all bidders	The evaluation of bids shall be based on the documents, credentials, experience references, and information submitted by the bidder as part of its bid response on or before the bid submission deadline. Any new credential, experience reference, document, or supporting evidence that was not originally submitted with the bid may, at the Bank's discretion, not be accepted or considered during the evaluation process. Bidders are therefore advised to ensure that all required documents and supporting evidence are submitted along with the bid. The Bank shall evaluate the bid based on the	Refer Section 10.1 – Preliminary Scrutiny

Addendum 1

#	Pre Bid/RFP Reference	Page No.	Published RFP Clause	Updated Clause	Revised RFP Reference
RFP					
				documents submitted and the Bank's decision regarding the adequacy, relevance, interpretation, compliance, and evaluation of the submitted documents and information shall be final, conclusive, and binding on all bidders.	
28.	Section 10.3 Eligibility Evaluation Criteria	129	Entire 10.2 Technical Evaluation Criteria	Refer Section 10.2 Eligibility Evaluation Criteria of Updated RFP.	10.3 Eligibility Evaluation Criteria
29.	Section 10.3 Technical Evaluation Criteria – Note (new)	129	New note.	Note: The documents requirement remains same for the technical evaluation, refer the Section 10.2 Eligibility Evaluation Criteria.	Refer Section 10.3 – Technical Evaluation Criteria – Note
30.	Section 10.3 Technical Evaluation Criteria	129	Entire 10.3 Technical Evaluation Criteria	Refer Section 10.3 Technical Evaluation Criteria of Updated RFP.	10.3 Technical Evaluation Criteria
31.	Section 10.4 Commercial Evaluation Criteria, Point 8	136	At the sole discretion and determination of the bank, the bank may add any other relevant criteria for evaluating the proposals received in response to this RFP.	At the sole discretion and determination of the bank, the bank may add any other relevant criteria for evaluating the proposals received in response limited to the terms defined in this RFP without material impact.	Refer Section 10.4 – Commercial Evaluation Criteria, Point 8
32.	14.1 Assignment & Subcontracting	159	New Point 3 is added	3. All Bidder's personnel deployed on the project shall be on Bidder's payroll. The Bidder shall submit the relevant EPFO and ESIC details/documents of each of the personnel to the Bank for verification of their employment status.	14.1 Assignment & Subcontracting

Addendum 1

#	Pre Bid/RFP Reference	Page No.	Published RFP Clause	Updated Clause	Revised RFP Reference
RFP					
33.	Section 11 Right to Reduce / Descope Solution Components Prior to Award	136-137	Entire Section 11 : Right to Reduce / Descope Solution Components Prior to Award	Clause Stands Deleted	Refer Section 11 – Right to Reduce / Descope Solution Components Prior to Award (Clause Stands Deleted)
34.	Section 13.1 Service Level Agreement, Point 16	142	If any customer-facing application, Core Banking System (CBS), regulatory application, statutory application, or other critical banking service becomes unavailable, disrupted, or degraded due to an issue attributable to the Core Firewall or Perimeter Firewall or solution(s) supplied under this RFP, and the incident is classified by the Bank as a Critical-Level Incident, the Bank may impose an additional penalty over and above the standard SLA penalties. Where such an incident remains unresolved for more than 120 minutes, an additional penalty of 0.5% of the monthly maintenance charges shall be levied for every subsequent hour or part thereof until the issue is resolved and normal services are restored.	Clause stands deleted	Refer Section 13.1 – Service Level Agreement (Point 16 of the published RFP deleted; subsequent points renumbered)
35.	Section 13.1 Service Level Agreement – Availability Measurements (Cyber Security Solutions and IT	146	99.90%	Section 13.1 Service Level Agreement – Availability Measurements (Cyber Security Solutions and IT Infrastructure), Minimum Service Level	Refer Section 13.1 – Service Level Agreement, Availability Measurements table

Addendum 1

#	Pre Bid/RFP Reference	Page No.	Published RFP Clause	Updated Clause	Revised RFP Reference
RFP					
	Infrastructure), Minimum Service Level				
36.	Section 14.25 Exit Management (new clause)	168	New clause.	Refer Section 14.25 – Exit management	Refer Section 14.25 – Exit Management
37.	Section 16.21.2 Volumetrics – Solution-wise Requirements	258-261	Table (# 1 to 16).	Refer Annexure 21	Refer Section 16.21.2 – Volumetrics & Storage Solution-wise Requirements
38.	Section 16.21.3 Deployment and Data Retention	261	Retention requirements for online/searchable, backup and long-term storage (LTS) data, including the retention table.	Refer Annexure 21	Refer Section 16.21.3 – Deployment and Data Retention
39.	Section 16: Annexure	171	Updated Annexures	Annexure 1, Annexure 2, Annexure 3, Annexure 4, Annexure 5, Annexure 6, Annexure 8, Annexure 9	Refer Section 16.1, 16.2,16.3,16.4,16.5,16.8,16.9
40.	Annexure 22: Client References Format	263-265	Annexure 22: Client References Format Solution/service list includes 'Anti-Phishing Services'.	Annexure 22 Updated as Annexure 22A	Refer Section 16.22 – Annexure 22A: Bidder's Client References Format
41.	Annexure 22B: OEM Self-Declaration For Implementation Experience (new annexure)	–	New annexure.	New annexure added – refer Annexure 22B of the revised RFP.	Refer Section 16.23 – Annexure 22B: OEM Self-Declaration For Implementation Experience

Addendum 1

#	Pre Bid/RFP Reference	Page No.	Published RFP Clause	Updated Clause	Revised RFP Reference
RFP					
42.	Annexure 25: List of currently available reports	268	Annexure 25: List of currently available reports NEXTGEN SOC Solution & services and the relevant Project from the list of solution sought by bank	Annexure 25 Updated	Refer Section 16.26 – Annexure 25: Indicative List of Reports to be Provided to the Bank
43.		–	New annexure.	New annexure added – Annexure 26 , Annexure 27, Annexure 28, Annexure 29, Annexure 30, Annexure 31, Annexure 32, Annexure 33, Annexure 34,	Refer Section 16 of the Updated RFP

Section 4: Modification in Appendix

Appendix 1A

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specfications	Revised RFP Reference
44.	Appendix 1A – Cloud Deployment Requirement ("All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution")	All Cloud/SaaS solutions	Minimum Specifications (all serial numbers).	Refer Section 15.1 – Appendix 1A: Cloud Deployment Requirement (as replaced by Section 3 of this Addendum)
45.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: NDR, S.No. 3	NDR	Complete Solution and Specifications	The Network Detection and Response (NDR) requirement has been deleted. Accordingly, the corresponding capabilities should be demonstrated through the proposed XDR platform, refer revised XDR specification Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: XDR
46.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: SIEM, S.No. 18	SIEM, S.No. 18	The proposed solution shall provide cloud-native high availability and redundancy mechanisms to tolerate failures of underlying infrastructure components without disruption to security monitoring and operational capabilities. The solution shall provide automated failover and service continuity within the cloud environment through the CSP's native availability and resiliency capabilities	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: SIEM, S.No. 18

Addendum 1

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specfications	Revised RFP Reference
47.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: SIEM, S.No. 131	SIEM, S.No. 131	The proposed cloud-delivered solution shall provide secure multi-tenant architecture with appropriate logical tenant isolation, encryption in transit and at rest, secure authentication, MFA, granular RBAC, audit logging and protection of Bank security data in accordance with the approved service architecture, security controls and SLA.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: SIEM, S.No. 131
48.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: SIEM, S.No. 134	SIEM, S.No. 134	New Point	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: SIEM, S.No. 134
49.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: XDR, S.No. 43	XDR, S.No. 43	The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature or through seamless integration with a third-party sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: XDR, S.No. 43
50.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Decoy, S.No. 20	Decoy, S.No. 20	Includes an algorithm for automated rule creation that integrates with SOAR platforms, enabling real-time blocking of attacker IPs based on threat intelligence gathered from decoys. Features a customizable Generative AI model to assist security analysts with contextual insights, investigative support, and proactive security measures.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Decoy, S.No. 20

पंजाब एण्ड सिंध बैंक *Email: soc.tender@psb.bank.in*		***Punjab & Sind Bank*** *Email: soc.tender@psb.bank.in*

Addendum 1

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specfications	Revised RFP Reference
51.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Decoy, S.No. 25	Decoy, S.No. 25	The proposed solution shall be delivered as a cloud-based/SaaS platform hosted within the CSP environment. The bidder shall provision and size the required cloud compute, storage, network, and other platform resources to meet the Bank's performance, scalability, High Availability (HA), service continuity, and Disaster Recovery (DR) requirements in accordance with the applicable Cloud Deployment Model.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Decoy, S.No. 25
52.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Decoy, S.No. 26	Decoy, S.No. 26	The proposed solution shall support multiple types of decoys, emulation of common network devices, including TCP port emulation. Network IT Decoys emulation of full OS Decoy supports real Operating Systems of Windows 7 / 10 / server 2016/2019, Linux, (Ubuntu/CentOS), ERP/POS/DB/WEB	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Decoy, S.No. 26
53.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 1.4	ITDR, S.No. 1.4	Identity Threat Detection Solution must find and present high-risk attack pathways to critical IT assets	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 1.4
54.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 1.6	ITDR, S.No. 1.6	Identity Threat Detection Solution should must automatically prioritize and remediate the riskiest identities to preemptively cut off what attackers need (and expect to find) to move undetected within the network.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 1.6
55.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 2.3	ITDR, S.No. 2.3	The ITDR solution shall identify and assess exposed, improperly stored, or compromised credentials associated with user, privileged, service, and administrative identities on endpoints	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 2.3

Addendum 1

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specfications	Revised RFP Reference
56.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 2.4	ITDR, S.No. 2.4	Identity Threat Detection Solution should Identify, Misconfigured accounts, Legacy app accounts, Stale accounts, password policy violations, Kerberoastable credentials, unmanaged user accounts, unmanaged service accounts	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 2.4
57.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 2.5	ITDR, S.No. 2.5	Identity Threat Detection Solution should Provide continuous monitoring and customizable, automated business rules to eliminate security policy violations, such as: • Stored credentials to sensitive assets • Local-admin accounts • Cached credentials stored in browsers, Windows and other systems	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 2.5
58.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 2.6	ITDR, S.No. 2.6	Identity Threat Detection Solution should be capable of creating tickets in the organization's ITSM system for vulnerabilities that cannot be safely addressed through automation, allowing them to be managed and remediated through established IT operational workflows.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 2.6
59.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 2.7	ITDR, S.No. 2.7	Identity Threat Detection Solution should be available through rack-mountable on-premise deployment	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 2.7
60.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 2.15	ITDR, S.No. 2.15	Identity Threat Detection controls should be able to automatically discover and flag hidden or shadow Tier 0 assets	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 2.15
61.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 2.17	ITDR, S.No. 2.17	Identity Threat Detection Solution should be able to pull and analyze identity data from AD, Entra ID, identity stores, PAM systems	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 2.17

Addendum 1

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specfications	Revised RFP Reference
62.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 2.18	ITDR, S.No. 2.18	Identity Threat Detection Solution should integrate with the organization's ITSM and software distribution systems to facilitate the collaboration between security and IT teams	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 2.18
63.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 3.4	ITDR, S.No. 3.4	The Identity Threat Detection Solution should integrate with compatible endpoint/extended detection solution to capture screen recordings or screenshots during active attacker sessions, as part of advanced forensic evidence collection	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 3.4
64.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 3.5	ITDR, S.No. 3.5	The Identity Threat Detection Solution should integrate with compatible network detection solution to support collection of PCAP data to support network-level visibility of the incident	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 3.5
65.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 3.7	ITDR, S.No. 3.7	Identity Threat Detection Solution should, as part of its forensic data collection process, include detailed attack path information, including the protocols leveraged during the attack.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 3.7
66.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 3.8	ITDR, S.No. 3.8	Identity Threat Detection Solution should collect user and computer information from Active Directory as part of its forensic data gathering to enhance context and assess risk exposure.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 3.8
67.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 3.9	ITDR, S.No. 3.9	Identity Threat Detection solution should detect an adversary's attempt to move laterally toward the organization's key assets using as many hosts (Windows, Mac, or Linux) as possible in the organization without requiring a persistent agent.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 3.9

Addendum 1

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specfications	Revised RFP Reference
68.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 3.10	ITDR, S.No. 3.10	Identity Threat Detection Solution should collect user and computer information from Active Directory as part of its forensic data gathering to enhance context and assess risk exposure. detect at the earliest point in the attack, post initial compromise as the attacker is first attempting to move laterally and escalate privilege.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 3.10
69.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 3.11	ITDR, S.No. 3.11	Identity Threat Detection Solution should collect user and computer data from Active Directory during forensic data gathering to improve context and evaluate risk exposure, while ensuring that all deception techniques remain hidden from legitimate users.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: ITDR, S.No. 3.11
70.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 1	CTEM, S.No. 1	The solution should collect intelligence from multiple languages and relevant regional sources, with support for multilingual threat intelligence processing and analysis.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 1
71.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 2	CTEM, S.No. 2	The solution should support translation or interpretation of collected intelligence into English	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 2
72.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 7	CTEM, S.No. 7	Each intelligence item should include metadata such as date, author, source, and pre-classification of raw data	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 7
73.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 10	CTEM, S.No. 10	Analysts should perform threat hunting activities to find findings outside of the platform	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 10

Addendum 1

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specfications	Revised RFP Reference
74.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 12	CTEM, S.No. 12	The solution should provide general and industry-related cyber intelligence reports on threat landscape trends, at least twice a month	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 12
75.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 18	CTEM, S.No. 18	The solution should provide comprehensive threat actor attribution including known identities, motivations, historical activity, TTPs, associated infrastructure, and MITRE ATT&CK mapping	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 18
76.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 19	CTEM, S.No. 19	The solution should detect compromised credentials for employees and VIPs, exposed payment card information, and aggregate data from known breach databases in real time	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 19
77.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 20	CTEM, S.No. 20	The solution should support IoC enrichment — allowing submission of IPs, domains, and hashes to receive contextual threat intelligence and threat actor attribution	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 20
78.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 21	CTEM, S.No. 21	The solution should support threat actor interaction via vendor analysts (e.g., engaging via dark web avatars) to gather additional intelligence	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 21
79.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 22	CTEM, S.No. 22	The solution should support scanning and reputation analysis of submitted IP addresses	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 22
80.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 23	CTEM, S.No. 23	The solution should support reporting of confirmed malicious or phishing assets to relevant external platforms and authorities, where such reporting is supported and authorized.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 23

Addendum 1

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specfications	Revised RFP Reference
81.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 24	CTEM, S.No. 24	The solution should provide pre-built bidirectional integrations with SIEM, SOAR, ticketing (Manage Engine), and threat intelligence platforms	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 24
82.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 30	CTEM, S.No. 30	The solution shall provide automated validation of identified exposures, where technically applicable and authorized by the Bank, using controlled, non-destructive testing or equivalent validation mechanisms to determine whether the identified exposure is genuinely exploitable or materially exposed.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 30
83.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 33	CTEM, S.No. 33	The solution should validate that a vulnerability is actually exploitable or otherwise materially exposed (active exposure validation)	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 33
84.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 35	CTEM, S.No. 35	The solution should detect malicious files, reconnaissance activity, automated attack tools, and target lists	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 35
85.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 38	CTEM, S.No. 38	The solution should be deployed agentlessly, without requiring sensors or agents on endpoints, servers, or network appliances	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 38
86.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 45	CTEM, S.No. 45	The solution should support manual IoC management operations	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 45

Addendum 1

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specfications	Revised RFP Reference
87.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 47	CTEM, S.No. 47	The solution should support cross-platform IoC enforcement across the security stack	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 47
88.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 48	CTEM, S.No. 48	The solution should assess and harden network, endpoint, and operating system security controls	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 48
89.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 49	CTEM, S.No. 49	The solution should provide a private exposure map of the organization's attack surface	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 49
90.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 50	CTEM, S.No. 50	The solution should support custom protections tailored to the organization's environment	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 50
91.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 51	CTEM, S.No. 51	The solution should apply virtual patching/compensating controls/exposure mitigation mechaism to the firewall and other security systems through integration with relevant security controls.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 51
92.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 59	CTEM, S.No. 59	The solution should support API-based remediation, notification or workflow integration with relevant security controls	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 59

Addendum 1

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specfications	Revised RFP Reference
93.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 60	CTEM, S.No. 60	The solution should support automated remediation workflows	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 60
94.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 62	CTEM, S.No. 62	The solution should leverage compensating controls and layered defense strategies to manage threats proactively	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 62
95.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 65	CTEM, S.No. 65	The solution should aim to reduce Mean Time to Remediate (MTTR) and labor costs	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 65
96.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 66	CTEM, S.No. 66	The solution should maximize ROI from existing security tools by optimizing the security posture	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Continuous Threat Exposure Management (CTEM), S.No. 66
97.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 67	CTEM, S.No. 67	The vendor to provide a mechanism to report security incidents identified through the platform and receive prompt response and guidance from the incident response team	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: CTEM, S.No. 67

Addendum 1

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specfications	Revised RFP Reference
98.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Cloud Security (CSPM), S.No. 4	CSPM, S.No. 4	The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud environment like AWS/Azure/GCP/Meghdoot, AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Cloud Security (CSPM), S.No. 4
99.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Cloud Security (CSPM), S.No. 9 (sub-point)	CSPM, S.No. 9	○ Automatic, in-product remediation via the Cloud Service Provider (CSP) API (1-click)	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Cloud Security (CSPM), S.No. 9 (sub-point)
100.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Cloud Security (CSPM), S.No. 25	CSPM, S.No. 25	The solution must provide an self-service portal for engineers. The admin portal should be able to define the eligibility for users and groups, based on role, scope and duration. The solutuon should provide approval workflow and audit logs	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Cloud Security (CSPM), S.No. 25
101.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Cloud Security (CSPM), S.No. 26	CSPM, S.No. 26	The propose solution should have Cloud Native Application Protection (CNAPP) as inbulit solution or additional solution that can provide security through a deep technological integration and strategic business alliance, delivering holistic security solution.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Cloud Security (CSPM
102.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Cloud Security (CSPM), S.No. 27	CSPM, S.No. 27	The proposed CNAPP solution should provides bank with more context to drive actionable security and smarter prevention, from code-to-cloud, across the application lifecycle.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Cloud Security (CSPM

Addendum 1

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specfications	Revised RFP Reference
103.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Cloud Security (CSPM), S.No. 28	CSPM, S.No. 28	The proposed CNAPP solution should must have below capabilities and required licenses from day one > CSPM - Compliance and governance for the full cloud stack > CIEM - Least Privildge Access/Excessive Permission and Identity Management > CWP - Protection/Response across all the running cloud workloads > KSPM - Container Security and compliance in the cloud and on-prem > CDR - detect, analyse and respond across the cloud environment > AISPM - Visbility and security for AI workloads, services and data used in training and inference >CTEM -- Continuous Threat Exposure Management (CTEM)	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Cloud Security (CSPM
104.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: CNAPP, S.No. 59	CNAPP, S.No. 59	The solution shall support high availability and service continuity appropriate to the proposed deployment architecture and shall provide mechanisms for recovery of relevant configurations, policies and security information.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: CNAPP, S.No. 59
105.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: CWPP, S.No. 47	CWPP, S.No. 47	The solution shall support high availability and service continuity appropriate to the proposed deployment architecture and shall provide mechanisms for recovery of relevant configurations and security policies.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: CWPP, S.No. 47
106.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: CWPP, S.No. 48	CWPP, S.No. 48	The solution shall provide mechanisms to identify the protection health/status of onboarded workloads, including agent, connector or communication health where applicable.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: CWPP, S.No. 48

Addendum 1

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specfications	Revised RFP Reference
107.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Vulnerability Assessment & vulnerability lifecycle Management (VA-VM), S.No. 1	VA-VM, S.No. 1	The proposed solution shall be deployable entirely on-premises and shall not require any cloud-hosted component, external service, or Internet connectivity for its core functionality, scanning, management, reporting, analytics, or product capabilities.	
108.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Vulnerability Assessment & vulnerability lifecycle Management (VA-VM), S.No. 45	VA-VM, S.No. 45	The solution shall integrate with enterprise CMDB, ITSM, SIEM, SOAR, PAM and NAC platforms through secure REST APIs.	
109.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Vulnerability Assessment & vulnerability lifecycle Management (VA-VM), S.No. 48	VA-VM, S.No. 48	The solution shall support secure encrypted communication using TLS 1.3 and cryptographic modules compliant with FIPS 140-3 or equivalent internationally recognized standards.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Vulnerability Assessment & vulnerability lifecycle Management (VA-VM), S.No. 48
110.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Vulnerability Assessment & vulnerability lifecycle Management (VA-VM), S.No. 51	VA-VM, S.No. 51	The solution shall identify internet-facing assets and continuously monitor externally exposed services.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Vulnerability Assessment & vulnerability lifecycle Management (VA-VM), S.No. 51
111.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Vulnerability Assessment & vulnerability lifecycle Management (VA-VM), S.No. 56	VA-VM, S.No. 56	The solution shall support digitally signed and password-protected reports with configurable retention and archival.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Vulnerability Assessment & vulnerability lifecycle Management (VA-VM), S.No. 56
112.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Vulnerability Assessment & vulnerability lifecycle Management (VA-VM), S.No. 60	VA-VM, S.No. 60	The solution shall provide comprehensive REST APIs and webhook support for automation and integration with enterprise security platforms.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Vulnerability Assessment & vulnerability lifecycle Management (VA-VM), S.No. 60

Addendum 1

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specfications	Revised RFP Reference
113.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Vulnerability Assessment & vulnerability lifecycle Management (VA-VM), S.No. 73	VA-VM, S.No. 73	The solution shall support secure encrypted communication using TLS 1.3 and cryptographic modules compliant with FIPS 140-2, FIPS 140-3, or equivalent internationally recognized cryptographic standards, as applicable.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Vulnerability Assessment & vulnerability lifecycle Management (VA-VM), S.No. 73
114.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Vulnerability Assessment & vulnerability lifecycle Management (VA-VM), S.No. 87	VA-VM, S.No. 87	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Vulnerability Assessment & vulnerability lifecycle Management (VA-VM), S.No. 87
115.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Vulnerability Assessment & vulnerability lifecycle Management (VA-VM), S.No. 89	VA-VM, S.No. 89	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Vulnerability Assessment & vulnerability lifecycle Management (VA-VM), S.No. 89

Addendum 1

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specfications	Revised RFP Reference
116.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Vulnerability Assessment & vulnerability lifecycle Management (VA-VM), S.No. 91	VA-VM, S.No. 91	White-Label Reporting and Approval Workflow: The proposed solution shall support customizable/white-label security assessment reports, including organization-specific branding and configurable report content. The solution shall support role-based maker-checker workflow for report generation, review, approval, and controlled release of finalized reports.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Vulnerability Assessment & vulnerability lifecycle Management (VA-VM), S.No. 91
117.	Appendix 1A – Functional Compliance Sheet (Solutions), Sheet: Vulnerability Assessment & vulnerability lifecycle Management (VA-VM), S.No. 92	VA-VM, S.No. 92	Multi-Tenant Data Isolation: The proposed solution shall support secure multi-tenancy for managed-security/shared-service deployments, providing logical and access-controlled segregation of each customer's assets, credentials, scan configurations, findings, reports, and other security data. APIs and administrative interfaces shall enforce appropriate tenant-level authorization and data isolation.	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Vulnerability Assessment & vulnerability lifecycle Management (VA-VM), S.No. 92
118.	APPENDIX 1A Functional Compliance Sheet (Solutions), Sheet: Cloud Deployment Requirement		Existing Cloud Deployment Requirement	Refer Section 15.1 – Appendix 1A: Functional Compliance Sheet (Solutions), Sheet: Cloud Deployment Requirement

Appendix 1B

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specifications	Revised RFP Reference
119.	Appendix 1B – Technical Compliance Sheet (IT	Primary Storage S.No. 4	The proposed array should be configured using all NVMe drives on Industry standard RAID6 and should be able to deliver at least 1,50,000 IOPS (8K block size, 80% Read/20% Write) with minimal latency for both read & write IOs.	Refer Section 15.2 – Appendix 1B: Technical Compliance Sheet (IT Infrastructure), Primary Storage, S.No. 4

Addendum 1

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specifications	Revised RFP Reference
	Infrastructure), Primary Storage, S.No. 4		Mentioned performance numbers should be achieved with data reduction techniques like Compression & deduplication and data Encryption turned ON. OEM should submit the document / official sizing tool output stating the above-mentioned performance metrics capability of the proposed system. These performance numbers should be delivered after considering the overheads of deduplication, compression and encryption. The capacity to be configured as a single/multiple storage pool which should be accessible to both the controllers simultaneously for Read & Write operations.	
120.	Appendix 1B – Technical Compliance Sheet (IT Infrastructure), Primary Storage, S.No. 5	Primary Storage S.No. 5	Proposed storage solution should be offerred with minimum 2 controllers with minimum 256 GB DRAM Cache memory on the entire storage Solution. The solution should scale to atleast 512GB Cache memory by adding additional controller. The proposed array must protect data in cache during a manual power down or an unexpected power outage by vaulting to flash storage. The NVMe SSD capacity drives must not be used for any caching requirements of the storage. The caching requirements of storage must be factored separately	Refer Section 15.2 – Appendix 1B: Technical Compliance Sheet (IT Infrastructure), Primary Storage, S.No. 5
121.	Appendix 1B – Technical Compliance Sheet (IT Infrastructure), Primary Storage, S.No. 8	Primary Storage S.No. 8	The proposed array should be configured with at least 8 x 32Gbps & 8 x 10Gbps optical front-end ports & Proposed storage should support 100GbE backend.	Refer Section 15.2 – Appendix 1B: Technical Compliance Sheet (IT Infrastructure), Primary Storage, S.No. 8
122.	Appendix 1B – Technical Compliance Sheet (IT Infrastructure), Backup Software, S.No. 7	Backup Software S.No. 7	Should be able to archive ALL workloads (VMs, DBs, Files) backup data by moving it to another disk target with different hardware using NFS/S3 protocols for long term retention and all the licenses for backup software and backup storage must be provided on day 1.	Refer Section 15.2 – Appendix 1B: Technical Compliance Sheet (IT Infrastructure), Backup Software, S.No. 7
123.	Appendix 1B – Technical Compliance Sheet (IT Infrastructure), Backup Software, S.No. 8	Backup Software S.No. 8	The proposed backup solution must support provide Data protection, Replication, Encryption, Immutability, MFA (Multi-factor authentication) and archival to external NFS/S3 based storage from day 1 and all these licenses must be included.	Refer Section 15.2 – Appendix 1B: Technical Compliance Sheet (IT Infrastructure), Backup Software, S.No. 8

Addendum 1

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specifications	Revised RFP Reference
124.	Appendix 1B – Technical Compliance Sheet (IT Infrastructure), Backup Storage/Appliance, S.No. 16	Backup Storage/Appliance S.No. 16	The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data over a secure, API-based disk-to-disk (D2D) connection.	Refer Section 15.2 – Appendix 1B: Technical Compliance Sheet (IT Infrastructure), Backup Storage/Appliance, S.No. 16
125.	Appendix 1B – Technical Compliance Sheet (IT Infrastructure), Backup Storage/Appliance, S.No. 18	Backup Storage/Appliance S.No. 18	Proposed Disk Based Appliance/backup storage should have the capability to tier backup data to an external cloud storage (on premise / public cloud) and the required licenses must be provided on day 1. Proposed backup solution with storage/appliance should have redundant components (Backup Storage - controllers, Power , fans etc. and Backup Appliance - Power , fans etc.) , HA mechanism in place to avoid Single Point of Failure and should have minimum of 4x16/32 GB FC ports & 2x32G ports on each controller for Host connectivity. Proposed Backup Solution should have minimum 4x scalability of the current quoted capacity for future growth.	Refer Section 15.2 – Appendix 1B: Technical Compliance Sheet (IT Infrastructure), Backup Storage/Appliance, S.No. 18
126.	Appendix 1B – Technical Compliance Sheet (IT Infrastructure), Backup Storage/Appliance, S.No. 25	Backup Storage/Appliance S.No. 25	The Proposed Appliance/Backup Storage must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism	Refer Section 15.2 – Appendix 1B: Technical Compliance Sheet (IT Infrastructure), Backup Storage/Appliance, S.No. 25
127.	Appendix 1B – Technical Compliance Sheet (IT Infrastructure), Long Term Storage, S.No. 1	Long Term Storage S.No. 1	Proposed storage would be proposed for long retention of Backup data (Protocol- NAS/CIFS/SMB/S3/SAN storage (Protocol- iSCSI)	Refer Section 15.2 – Appendix 1B: Technical Compliance Sheet (IT Infrastructure), Long Term Storage, S.No. 1
128.	Appendix 1B – Technical Compliance Sheet (IT Infrastructure), Primary Storage (new clause)		New clause.	Refer Section 15.2 – Appendix 1B: Technical Compliance Sheet (IT Infrastructure), Primary Storage (new clause)
129.	Appendix 1B – Technical Compliance Sheet (IT Infrastructure), Backup Storage/Appliance (new clause)	Backup Storage/Appliance	New clause.	Refer Section 15.2 – Appendix 1B: Technical Compliance Sheet (IT Infrastructure), Backup Storage/Appliance (new clause)
130.	Appendix 1B – Technical Compliance Sheet (IT	Long Term Storage	New clause.	Refer Section 15.2 – Appendix 1B: Technical Compliance Sheet (IT

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specifications	Revised RFP Reference
	Infrastructure), Long Term Storage (new clause)			Infrastructure), Long Term Storage (new clause)

Appendix 1C

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specifications	Revised RFP Reference
131.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Brand abuse	Brand Abuse	Complete Specification and Scope	The Completed specification of Brand Abuse Stands deleted. Please refer Digital Risk Management Specifications Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet (Services), Sheet: Digital Risk Management
132.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Brand abuse	Anti - Phishing	Complete Specification and Scope	The Completed specification of Anti-Phishing Stands deleted. Please refer Digital Risk Management Specifications Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet (Services), Sheet: Digital Risk Management
133.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Threat Intelligence Feed, S.No. 7	Threat Intelligence Feed S.No. 7	The portal must provide IoC lookups (reputation & analysis). This capability should give insights to understand how malware files act and communicate. The TI tool should detonates files in virtual controlled environments to trace their activities and communications, producing detailed reports including	Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet (Services), Sheet: Threat Intelligence Feed, S.No. 7

Addendum 1

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specifications	Revised RFP Reference
			opened, created and written files, created mutexes, registry keys set, contacted domains, URL lookups, etc. This execution activity should be indexed in a faceted fashion in order to allow for instantaneous lookups.	
134.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Threat Intelligence Feed, S.No. 13	Threat Intelligence Feed S.No. 13	TI portal must have capability to search that allows users to ask natural language questions to get a generative AI-powered/AI-driven overview on their question	Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet (Services), Sheet: Threat Intelligence Feed, S.No. 13
135.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Threat Intelligence Feed, S.No. 14	Threat Intelligence Feed S.No. 14	TI provider must have capability to create YARA rules against URLs, domains and IP addresses and hunt for new network indicators that match certain metadata.	Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet (Services), Sheet: Threat Intelligence Feed, S.No. 14
136.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Threat Intelligence Feed, S.No. 15	Threat Intelligence Feed S.No. 15	Threat intelligence provider must provide the relationships graph to understands the relationship between files, URLs, domains, IP addresses and other items encountered in an ongoing investigation (threat actors, campaigns, malware families, etc.). With it, TI analyst can pivot intelligently over any of the malware artifacts in your graph and synthesize your findings into a threat map.	Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet (Services), Sheet: Threat Intelligence Feed, S.No. 15
137.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Threat Intelligence Feed, S.No. 16	Threat Intelligence Feed S.No. 16	The provider must provide the curated Strategic Reporting generated by threat intelligence analysts in the following areas: a) Industry: Reports on threats specific to an industry vertical, considering various adversary motivations. b) Region / Country profile: Reports on threats targeting a particular country or geographic region, across different adversary motivations.	Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet (Services), Sheet: Threat Intelligence Feed, S.No. 16

Addendum 1

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specifications	Revised RFP Reference
			c) Trends & Forecasting: Analysis of threat actor tactics, trends, and types of threat activity, potentially including historical reviews and predictions. d) Executive Perspective: Analysis about cyber threats relevant to events or business circumstances, geared toward a strategic leadership audience. This report type also includes Intelligence-at-a-Glance reports, which provide a weekly snapshot into newly produced reports, blogs, webinars; as well as some insight into customer interests based on top search terms and most read reports.	
138.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Threat Intelligence Feed, S.No. 17	Threat Intelligence Feed S.No. 17	The provider must provide curated details on various aspects of adversary activities, with a focus on their methods and behaviors. Including: a) Actor Profile: In-depth look into a specific threat actor's tactics, techniques, and procedures. b) TTP Deep Dives: Detailed analysis into a threat actor and the tactics, techniques, and procedures (TTPs) they use to achieve specific goals. c) Event Coverage / Implication: Analysis on the implications of a recent event or campaign conducted by a threat actor. d) Malware Profile: Technical analysis of a representative sample of a code family. This report type typically includes file characteristics, host- and network-based indicators, configuration information, and details of code execution.	Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet (Services), Sheet: Threat Intelligence Feed, S.No. 17

Addendum 1

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specifications	Revised RFP Reference
139.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Threat Intelligence Feed, S.No. 21	Threat Intelligence Feed S.No. 21	New Point	The threat feeds must provide relevant threat intelligence feeds, including IP Reputation, Malicious URL, Phishing URL, Botnet C&C URL, and malicious/suspicious Domains, that must be updated at least once every 1 hour to 4 hours and every 1 week for CVEs and other relevant indicators, ensuring near real-time coverage of emerging threats.
140.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Attack Surface Management, S.No. 8	Attack Surface Management S.No. 8	The solution shall provide information on vulnerabilities, misconfigurations, insecure configurations, obsolete or unsupported technologies, applications, services, URLs, ports, network components, systems, databases and other relevant infrastructure that are publicly exposed or otherwise identifiable through authorized discovery and assessment activities.	Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet (Services), Sheet: Attack Surface Management, S.No. 8
141.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Attack Surface Management, S.No. 10	Attack Surface Management S.No. 10	The solution shall identify and provide relevant information on potentially exposed sensitive information associated with the Bank, including source-code references, code snippets, API information, credentials, keys and other security-relevant information, where such information is identifiable through publicly available sources, external attack-surface intelligence or other authorized discovery mechanisms.	Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet (Services), Sheet: Attack Surface Management, S.No. 10
142.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Attack Surface Management, S.No. 14	Attack Surface Management S.No. 14	All the software modules of the proposed solution should be latest as well as stable one and must have a general release date prior to the date of the submission of the proposal	Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet (Services), Sheet: Attack Surface Management, S.No. 14
143.	Appendix 1C – Functional Compliance Sheet (Services),	Attack Surface Management S.No. 35	Solution should have the feature to automatically create help desk ticket containing asset meta data, comments,	Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet

Addendum 1

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specifications	Revised RFP Reference
	Sheet: Attack Surface Management, S.No. 35		link back to the solution console and guidance. Ticket status should be automatically reflected in ASM console.	(Services), Sheet: Attack Surface Management, S.No. 35
144.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Attack Surface Management, S.No. 38	Attack Surface Management S.No. 38	Solution must have bi-directional, writetable API's that allow the organization to integrate data into the organization's existing security	Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet (Services), Sheet: Attack Surface Management, S.No. 38
145.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Dark Web Monitoring, S.No. 28.5	Dark Web Monitoring S.No. 28.5	Web Logs	Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet (Services), Sheet: Dark Web Monitoring, S.No. 28.5
146.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation, S.No. 16	Phishing Simulation S.No. 16	The bidder shall conduct Smishing exercises based on the frequency and number of target employees defined by the Bank. The bidder shall provide, maintain and manage an independent SMS gateway to perform smishing activity as per bank's requirement. The bidder shall maintain adequate security measures to protect Bank's data including any PII information submitted by users during the activity.	Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet (Services), Sheet: Phishing Simulation, S.No. 16
147.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation, S.No. 23.1	Phishing Simulation S.No. 23.1	The bidder shall perform review of Email solution twice in a year from Cert-IN empaneled organization and compliance verification shall be conducted within 2 months from the report submission.	Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet (Services), Sheet: Phishing Simulation, S.No. 23.1
148.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation, S.No. 23.2	Phishing Simulation S.No. 23.2	The platform should provide a separate dashboard for monitoring of DMARC/DNS Monitoring for Bank's Email solution.	Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet (Services), Sheet: Phishing Simulation, S.No. 23.2
149.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation, S.No. 23.3	Phishing Simulation S.No. 23.3	Support and Update	Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet (Services), Sheet: Phishing Simulation, S.No. 23.3

Addendum 1

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specifications	Revised RFP Reference
150.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation, S.No. 23.4	Phishing Simulation S.No. 23.4	The bidder should provide 24*7 support (over call) for any kind of issue in functionality/performance/integration of the platform during the entire tenure of contract. In case, the issue is not resolved for more than 8 hours, support personnel should visit Bank's CISO Office at Mumbai or at Hyderabad to resolve the issue. The bidder shall provide the details of support team and escalation matrix for immediate assistance to bank's team for any issue.	Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet (Services), Sheet: Phishing Simulation, S.No. 23.4
151.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation, S.No. 23.5	Phishing Simulation S.No. 23.5	The bidder should perform updation of new features and upgradation of on-premise platform automatically from time-to-time.	Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet (Services), Sheet: Phishing Simulation, S.No. 23.5
152.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation, S.No. 23.7	Phishing Simulation S.No. 23.7	For Phishing activity, the bidder should not store any bank data in vendor location, data storage shall be restricted only on Bank network. The bidder should ensure that the data at rest and in motion shall be encrypted.	Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet (Services), Sheet: Phishing Simulation, S.No. 23.7
153.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Continuous Automated Red Teaming (CART), S.No. 29	CART S.No. 29	The Attack playbooks must emulate a specific adversary TTP and threat actors to test for potential risks.	Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet (Services), Sheet: Continuous Automated Red Teaming (CART), S.No. 29
154.	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Continuous Automated Red Teaming (CART), S.No. 33	CART S.No. 33	The solution must have the ability to create custom active attack playbooks based on Threat Intelligence of Threat Actor and their TTPs	Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet (Services), Sheet: Continuous Automated Red Teaming (CART), S.No. 33
155.	Appendix 1C – Functional Compliance Sheet (Services),	CART S.No. 36	Solution should perform assessment of security controls related to email security, WAF security and endpoint	Refer Section 15.3 – Appendix 1C: Functional Compliance Sheet

Addendum 1

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specifications	Revised RFP Reference
	Sheet: Continuous Automated Red Teaming (CART), S.No. 36		security for known vulnerabilities, misconfigurations, implementation issues and any other security gaps	(Services), Sheet: Continuous Automated Red Teaming (CART), S.No. 36

ੴ ਸ੍ਰੀ ਵਾਹਿਗੁਰੂ ਜੀ ਕੀ ਫ਼ਤਹਿ

Punjab & Sind Bank

(A Govt. of India Undertaking)

Where service is a way of life

REQUEST FOR PROPOSAL

FOR

SELECTION OF BIDDER FOR SUPPLY INSTALLATION, IMPLEMENTATION, MAINTENANCE & MANAGEMENT OF NEXTGEN SOC & RELATED SERVICES

BID NO: PSB/ HO-CISO CELL/2026-27/RFP_01 DATED 09/09/2026

STAFF TRAINING CENTRE PUNJAB AND SIND BANK

Punjab & Sind Bank, CISO cell 3rd Floor,

B-8/232, Naharpur Village Rd, Pocket 8, Sector 3B,

Rohini, Delhi, 110085

1 Contents

1 KEY INFORMATION 8
2 GLOSSARY 11
3 DISCLAIMER 14
4 INTRODUCTION 15
5 PROJECT OBJECTIVE 15
6 INSTRUCTION TO BIDDER 15
6.1 Language of the Bid 15
6.2 Bid Currency & Price Structure 16
6.3 Bid System Offer 16
6.4 Two Bid System: 16
6.4.1 Preparation for Bids: 16
6.5 Cost of Preparation 18
6.6 Technical Normalization of Bids 18
6.7 Submission of Bid and communication 19
6.8 Late bids 19
6.9 Modifications and/ or Withdrawal of Bids 19
6.10 Earnest Money Deposit (EMD): 20
6.11 Performance Bank Guarantee (PBG) 21
6.12 No commitment to accept lowest or any bid 21
6.13 Right To Accept Any Bid and To Reject Any OR All Bids/ Cancellation of Tender process 21
6.14 Correction of Errors 22
6.15 Soft copy of tender document 23
6.16 Bid validity period 23
6.17 Pre-bid meeting 23
6.18 Amendment to RFP Contents 24
6.19 Disqualification 24
6.20 Fixed Price 24
6.21 Project Execution 24
6.22 Confidentiality of the Bid Document 24
7 SCOPE OF WORK 25
7.1 Scope and Objectives 25
7.2 Solution & Services Deployment Model and Their HA Requirement 29
7.2.1 Solutions – Master Deployment Matrix 29
7.2.2 Services 29
7.2.3 Deployment Model Definition 29
7.2.4 Deployment Architecture 29

7.3 Functional Requirements - Solutions 29
7.3.1 Security Information and Event Management 29
7.3.2 SOAR (Security Orchestration, Automation, & Response) 32
7.3.3 UEBA (User and Entity Behavior Analytics) 33
7.3.4 Extended Detection and Response (XDR) 33
7.3.5 Network detection and response (NDR) 34
7.3.6 Decoy/HoneyPOT 34
7.3.7 Threat Intelligence Platform 35
7.3.8 Vulnerability assessment (VA) & vulnerability lifecycle management 36
7.3.9 Identity Threat Detection & response 36
7.3.10 Application security testing Tool 38
7.3.11 Cloud Security (CSPM) Tool 38
7.3.12 Cloud-Native Application Protection Platform (CNAPP) 40
7.3.13 Cloud Workload Protection Platform (CWPP) 41
7.3.14 Continuous Threat Exposure Management (CTEM) Tool 42
7.4 Functional Requirement - Services (Offsite Services) 43
7.4.1 Breach Attack & Simulation 43
7.4.2 Continuous Automated Red Teaming Services 44
7.4.3 Attack surface management 44
7.4.4 Phishing Simulation 45
7.4.5 Anti-Phishing 45
7.4.6 Dark Web Monitoring 45
7.4.7 Threat Intelligence Feed 45
7.4.8 Threat Hunting Services 46
7.4.9 Brand Protection and Monitoring (Brand Abuse) 46
7.4.10 Digital Risk management 46
7.5 Bidder Responsibilities 47
7.6 OEM Responsibilities 48
7.6.1 Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder) 48
7.6.2 System Design - Activities are to be performed by Respective solution OEM (supported by bidder) 49
7.6.3 Development and Installation - Activities are to be performed by Respective Solution OEM (supported by bidder) 50
7.6.4 Documentation - Activities are to be performed by Respective solution OEM (supported by bidder) 51
7.6.5 Deployment and Go-Live - Activities are to be performed by Respective Solution OEM (supported by bidder) 51
7.6.6 Testing- Activities are to be performed by Respective solution OEM (supported by bidder) 52

7.6.7 Training- Activities are to be performed by Respective solution OEM (supported by bidder) 54
7.6.8 Security requirements - Activities are to be performed by Respective Solution OEM (supported by bidder) 56
7.7 On-cloud proposed solution OEM Responsibilities 57
7.8 Non-functional requirements 58
7.9 Delivery, Installation & Commissioning 59
7.10 Data Privacy 60
7.11 Warranty, ATS and AMC 60
7.12 Resource Requirement 61
7.12.1 Implementation Phase 61
7.12.2 Operations and Maintenance (O&M) Phase 61
7.12.3 Resource Management and Governance 62
7.12.4 Minimum Resource Count Deployment 63
7.12.5 Resource Deployment, Replacement and Governance 64
7.13 Facilities Management 66
7.13.1 Continual Improvement 69
7.14 DR Drill 72
7.15 NextGEN SOC operations: 72
7.16 OEM Services & Deployment (Architecture Assessment): 76
7.17 System recovery 76
7.18 IT Infrastructure requirements 78
7.18.1 Compute Infrastructure 80
7.18.2 Storage Infrastructure – Primary 81
7.18.3 Backup Infrastructure 81
7.18.4 Networking and Security Equipment: 82
7.18.5 Software 82
7.19 Other In-Scope Services 82
7.19.1 Other Scope Activity 82
7.19.2 Transition Management 83
7.19.3 Security Management 84
7.19.4 DR Setup - Activities are to be performed by Respective Solution OEM (supported by bidder) 85
8 CONTRACT PERIOD 85
9 PROJECT TIMELINES 86
10 EVALUATION CRITERIA 88
10.1 Preliminary Scrutiny 88
10.2 Eligibility Evaluation Criteria 89
10.3 Technical Evaluation Criteria 116

10.4 Commercial Evaluation Criteria 122
11 Right to Reduce / Descope Solution Components Prior to Award – Clause Stands Deleted. 123
12 PAYMENT TERMS 123
12.1 Product (Software) Cost 123
12.2 OEM Services Cost 125
12.3 Hardware Cost 125
12.4 ATS/subscription cost & AMC Cost 125
12.5 Facility Management (FM) Cost: 126
12.6 Other Cost 126
13 SERVICE LEVELS & PENALTIES 126
13.1 Service Level Agreement 126
13.2 Penalties 143
13.3 At-Risk Amount 144
14 TERMS AND CONDITIONS 145
14.1 Assignment & Subcontracting 145
14.2 Right to Alter quantities 145
14.3 Delays in the Bidder's Performance 145
14.4 Jurisdiction 145
14.5 Dispute Resolution 145
14.6 Notices 146
14.7 Legal Compliance 146
14.8 Digital Personal Data Protection Compliance 147
14.9 Non-Disclosure Agreement 147
14.10 Solicitation of Employees 147
14.11 Authorized Signatory 148
14.12 Confidentiality 148
14.13 Indemnity 148
14.14 Make in India 149
14.15 Force Majeure 149
14.16 Ownership & Retention of Documents: 150
14.17 Conflict of Interest: 150
14.18 Signing of Pre-Contract Integrity Pact: 150
14.19 Liquidated Damages 150
14.20 Intellectual Property Indemnity: 151
14.21 Limitation of Liability 151
14.22 Order Cancellation 152
14.23 Consequences of Termination 153

14.24 Audit by Third Party 154
14.25 Exit Management 155
15 APPENDIX 160
15.1 APPENDIX 1A: Functional Compliance Sheet (Solutions) 160
15.2 APPENDIX 1B: Technical Compliance Sheet (IT Infrastructure) 160
15.3 APPENDIX 1C: Functional Compliance Sheet (Services) 161
15.4 APPENDIX 2: Commercial Bill of material Sheet 161
15.5 APPENDIX 3: IT Infrastructure Virtual To Physical (V2P) Mapping 161
16 ANNEXURES 162
16.1 Annexure 1: Submission Checklist (on bidder's letterhead) 162
16.2 Annexure 2: Bidder's Information 167
16.3 Annexure 3: Tender Covering Letter 170
16.4 Annexure 4: Bid Security Declaration 172
16.5 Annexure 5: Pre-Qualification Criteria 174
16.6 Annexure 6: Acceptance/Compliance Certificate 199
16.7 Annexure 7: Minimum Local Content Certification 201
16.8 Annexure 8: Certification on OEM Requirements 202
16.9 Annexure 9: Escalation Matrix 206
16.9.1 Annexure 9A: Escalation Matrix - Bidder 206
16.9.2 Annexure 9B: Escalation Matrix – Respective security solution & service OEM 207
16.10 Annexure 10: Litigation Certificate 208
16.11 Annexure 11: Non-blacklisting undertaking 209
16.12 Annexure 12: Undertaking of Authenticity (on bidder's letterhead) 210
16.13 Annexure 13: Non-Disclosure Agreement 211
16.14 Annexure 14: Commercial Proposal Submission Checklist 217
16.15 Annexure 15: Bank Guarantee Format for Earnest Money Deposit 218
16.16 Annexure 16: Format of Performance Guarantee 220
16.17 Annexure 17 : Pre-contract integrity pact 223
16.18 Annexure 18: Compliance with FRS, TRS, SoW & SBOM (on respective OEM letterhead) 227
16.19 Annexure 19: Stack Confirmation Sheet - Undertaking for Proposed OEM Products 229
16.20 Annexure 20: S-BOM & C-BOM DETAILS of all the proposed Tool/solutions 231
16.21 Annexure 21: Sizing/Volumetrics, Data Retention and Current Infrastructure 233
16.21.1 Current IT assets 234
16.21.2 Volumetrics & Storage Solution-wise Requirements 235
16.21.3 Deployment and Data Retention 255
16.21.4 Solutions & Services – Master Deployment Matrix 260
16.22 Annexure 22A: Bidder's Client References Format 270

16.23 Annexure 22B: OEM Self-Declaration For Implementation Experience....272
16.24 Annexure 23: Pre-bid Query format 274
16.25 Annexure 24: Proposed Resources CV 275
16.26 Annexure 25: Indicative List of Reports to be Provided to the Bank....276
16.27 Annexure 26: Undertaking – Support & Launch Confirmation (on OEM's letterhead) 280
16.28 Annexure 27: Association with Bank....281
16.29 Annexure 28 Ownership Declaration and Contractual performance 283
16.30 Annexure 29: Contract Cancellation / Termination / Rescission / Revocation 284
16.31 Annexure 30: Compliance with Applicable Labour Laws 285
16.32 Annexure 31- Conflict of Interest and IT Security Vendor Restriction....286
16.33 Annexure 32 – OEM Functional Compliance Declaration....288
16.34 Annexure 33: Back-to-back support/backlining confirmation....289
16.35 Annexure 34: Insurance Surety Bond against EMD 290

1 KEY INFORMATION

Particulars	Details
Tender Title	RFP for Selection of bidder for supply installation, implementation, maintenance & management of NextGEN SOC & related services
Security Deposit/Earnest Money deposit	Rs. 4.25 Crore (INR Four Crore and Twenty-Five Lakh Only) Note: - Bidders who are eligible for EMD (Earnest Money Deposit) exemption as per GeM General Terms and Conditions (GeM 4.0, Version 1.25, dated 14th July 2025, Page 19) are required to submit a Bid Security Declaration in lieu of EMD. Please refer to RFP, Annexure 4: Bid Security Declaration for the prescribed format. This declaration must be duly filled, signed, and submitted along with the bid documents by vendors seeking the waiver of EMD submission. Failure to submit the Bid Security Declaration (where applicable) will result in the bid being treated as non-responsive.
Bid validity	180 days from the date of opening of the bid.
Performance Bank Guarantee	5% of Project Cost The selected bidder shall be responsible for providing the PBG for the duration of the contract (Including the extension) + claim period (12 months) of the Bank guarantees
Date of Publishing the tender on Bank's Website	As per GeM Portal
Last Date for submission of Pre-Bid Query	15/09/2026 at 5:00 PM a) Pre bid queries should be submitted as per Annexure 23 in MS-excel format. b) Queries should be submitted through GEM c) Queries must also be mailed to soc.tender@psb.bank.in only) quoting tender reference number in the subject. Subject of the email should be given as "Pre-Bid Queries for SELECTION OF BIDDER FOR SUPPLY INSTALLATION, IMPLEMENTATION, MAINTENANCE & MANAGEMENT OF NEXTGEN SOC & RELATED SERVICES". Queries arriving afterwards will not be entertained. d) Queries arriving afterwards will not be entertained/responded.
Date and Time for Pre-Bid Meeting	16/09/2026 at 11:00 AM • The Pre-Bid Meeting will be conducted online. Bidders who have submitted their pre-bid queries and the details of their authorized representatives (over an email), along with the requisite authorization, within the stipulated date and time for submission of pre-bid queries will be provided with the meeting link by the Bank. Such bidders are requested to attend the meeting through the link shared by the Bank.

Particulars	Details
	• A maximum of two (2) representatives from each bidder shall be permitted to attend the pre-bid meeting. The representatives must be duly authorized by the bidder through an authorization letter. The authorization letter shall be submitted through an email along with the pre-bid queries. • Those who are interested in participating the Prebid meeting should share the participant details to soc.tender@psb.bank.in • Link of the pre-bid meeting will be shared with participants having the authorization for whom the authorization letter has been shared Upon perusal of the same, the link / meeting id will be shared to the participant to participate in the virtual meeting.
Last Date and Time for submission of Bids	As per GeM Portal
Date and Time of Opening of Bids	As per GeM Portal
Date and time of online Commercial Bids	To be notified later to the qualifying bidders only.
Place of Opening of Bids	STAFF TRAINING CENTRE PUNJAB AND SIND BANK Punjab & Sind Bank, CISO cell 3rd Floor, B-8/232, Naharpur Village Rd, Pocket 8, Sector 3B, Rohini, Delhi, 110085
Submission of Bids	https://gem.gov.in/
Contact Persons for any clarifications/ Submission of Bids	Name: Santosh Kumar Neeraj (CISO) Contact No.: 7840053500 Email ID: soc.tender@psb.bank.in
Project Office Location	STAFF TRAINING CENTRE PUNJAB AND SIND BANK Punjab & Sind Bank, CISO cell 3rd Floor, B-8/232, Naharpur Village Rd, Pocket 8, Sector 3B, Rohini, Delhi, 110085
Other Details	1. No suggestions or queries shall be entertained after pre-bid meeting. 2. This document can also be downloaded from following website: https://punjabandsind.bank.in. Any Amendments, Modifications, Pre-Bid Replies, Clarifications & any communication etc. will be uploaded on the Bank's website (i.e. https://punjabandsind.bank.in) & https://gem.gov.in/ 3. No individual communication will be sent to the individual bidders.
Information for Online Participating: The following activities will be conducted online through the https://gem.gov.in/ website: 1. RFP document including all Annexures. 2. Addendums, Corrigendum and Clarifications to the RFP. 3. Submission of Technical Bid & Commercial Bid by the Bidder.	

Particulars	Details
4. Opening of Technical Bid 5. Opening Commercial Bid by the Bank. 6. Announcement of results, if any. Instructions: 1. Bidders who wish to participate will have to register with GeM Portal and follow respective guidelines. 2. In case of any clarification/ queries regarding online registration/ participation, Bidders may reach out to: Email: soc.tender@psb.bank.in	

* All MSMEs (Micro , Small and medium Enterprises) having registration as per provisions of the Public Procurement Policy for Micro, Small and Medium Enterprises i.e. District Industries Centre (DIC) or Khadi and Village Industries Commission (KVIC) or Khadi and Industries Board (KVIB) or Coir Board or National Small Industries Commission (NSIC) or directorate of Handicrafts and Handlooms or Udyog Aadhaar Memorandum or any other body specified by Ministry of MSME and Start-ups (recognized by DIPP) are exempted from submission of EMD amount only. Relevant Certificates should be submitted by the bidder in this regard to avail exemption.

Note:

If any of the dates given above happens to be Holiday in Banks in Delhi the related activity shall be undertaken on the next working day at the same time.

All Claims made by the Bidder will have to be backed by documentary evidence.

Bidders should submit bids well before time rather than wait for the last moment to avoid any technical glitches or networking issues etc. at their end.

Bidders are requested to use a reliable internet connection (data cable / broadband) to safeguard themselves. The bank is not responsible for telephone line glitches, internet response issues, hardware hangs etc. at bidder's end.

No Claim of any bidder shall be entertained, whatsoever for delayed submission of their bid at any stage because of any reason. Therefore, bidders are advised to submit their bids well before the scheduled time.

The tender document may also be downloaded from the Bank's official website also https://punjabandsind.bank.in

2 GLOSSARY

S. No.	Acronym	Abbreviation
1.	AI/ML	Artificial Intelligence / Machine Learning
2.	AMC	Annual Maintenance Cost
3.	API	Application Programming Interface
4.	ATS	Annual Technical Support
5.	BAS	Breach and Attack Simulation
6.	BCP	Business Continuity Planning
7.	BFSI	Banking, Financial Services, and Insurance
8.	BOQ	Bill of Quantity
9.	BRD	Business Requirements Document
10.	CBS	Core Banking Solution/System
11.	CBOM	Cryptographic Bill of Materials
12.	CCSA	Check Point Certified Security Administrator
13.	CEH	Certified Ethical Hacker
14.	CISA	Certified Information Systems Auditor
15.	CISO	Chief Information Security Officer
16.	CSP	Cloud Service Provider
17.	CSPM	Cloud Security Posture Management
18.	DAST	Dynamic Application Security Testing
19.	DAM	Database Activity Monitoring
20.	DB	Database
21.	DC	Data Centre
22.	DIC	District Industries Centre
23.	DLP	Data Loss Prevention
24.	DPDP	Digital Personal Data Protection
25.	DR	Disaster Recovery
26.	EMD	Earnest Money Deposit
27.	EOD/BOD	End of Day / Beginning of Day
28.	EPS	Event Per Second
29.	FMS	Facility Management System
30.	FRS	Functional Requirements Specification
31.	GCIA	GIAC Certified Intrusion Analyst
32.	GCIH	GIAC Certified Incident Handler
33.	GDPR	General Data Protection Regulation
34.	GUI	Graphical User Interface
35.	GST	Goods and Services Tax
36.	HIPS	Host Intrusion Prevention System
37.	HLD	High-Level Design
38.	IDAM	Identity and Access Management
39.	IOPS	Input/Output Operations Per Second
40.	IPS/IDS	Intrusion Prevention System/Intrusion Detection System
41.	IT	Information Technology
42.	ITSM	IT Service Management
43.	KVIC	Khadi and Village Industries Commission
44.	KVIB	Khadi and Village Industries Board

S. No.	Acronym	Abbreviation
45.	LAN	Local Area Network
46.	LDAP	Lightweight Directory Access Protocol
47.	LB	Load Balancer
48.	LLD	Low-Level Design
49.	LOI	Letter of Intent
50.	MTBF	Mean Time Between Failures
51.	MTTD	Mean Time to Detect
52.	MTTR	Mean Time to Respond/Repair
53.	MSME	Micro, Small and Medium Enterprises
54.	NAC	Network Access Control
55.	NBAD	Network Behaviours Anomaly Detection
56.	NDR	Network Detection and Response
57.	NGFW	Next-Generation Firewall
58.	NIST	National Institute of Standards and Technology
59.	NSIC	National Small Industries Corporation
60.	OEM	Original Equipment Manufacturer
61.	OOTB	Out Of the Box
62.	OS	Operating System
63.	PBG	Performance Bank Guarantee
64.	PII	Personally Identifiable Information
65.	PIM	Privileged Identity Management
66.	PSE	Public Sector Enterprise
67.	PSU	Public Sector Undertaking
68.	RACI	Responsible, Accountable, Consulted, Informed
69.	RBI	Reserve Bank of India
70.	RFP	Request for Proposal
71.	RPO	Recovery Point Objective
72.	RRB	Regional Rural Bank
73.	RTO	Recovery Time Objective
74.	SAN	Storage Area Network
75.	SAST	Static Application Security Testing
76.	SBOM	Software Bill of Materials
77.	SCD	Secured Configuration Document
78.	SDLC	Software Development Life Cycle
79.	SIEM	Security Information and Event Management
80.	SLA	Service Level Agreement
81.	SMS	Short Message Service
82.	SMTP	Simple Mail Transfer Protocol
83.	SNMP	Simple Network Management Protocol
84.	SOA	Service-Oriented Architecture
85.	SOC	Security Operations Centre
86.	SOAR	Security Orchestration, Automation and Response
87.	SOP	Standard Operating Procedure
88.	SRS	System Requirements Specification
89.	SSO	Single Sign-On

S. No.	Acronym	Abbreviation
90.	TAT	Turnaround Time
91.	TCC	Terms and Conditions of Contract
92.	TCO	Total Cost of Ownership
93.	TIP	Threat Intelligence Platform
94.	TTP	Tactics, Techniques, and Procedures
95.	UAT	User Acceptance Testing
96.	UEBA	User and Entity Behaviour Analytics
97.	ULA	Unlimited License Agreement
98.	UI/UX	User Interface / User Experience
99.	URL	Uniform Resource Locator
100.	VAPT	Vulnerability Assessment and Penetration Testing
101.	VPC	Virtual Private Cloud
102.	WAF	Web Application Firewall
103.	XDR	Extended Detection and Response
104.	VPN	Virtual Private Network

3 DISCLAIMER

1. The information contained in this Request for Proposal (RFP document) or any information provided subsequently to Bidder(s) whether verbally or in documentary form by or on behalf of the Bank, is provided to the Bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided. This document shall not be transferred, reproduced or otherwise used for purposes other than for which it is specifically issued.
2. This RFP is neither an agreement nor an offer and is only an invitation by the Bank to the interested parties for submission of bids. No contractual obligation whatsoever shall arise from the RFP process until a formal contract is executed by the duly authorized signatory of the Bank and the Bidder. The purpose of this RFP is to provide the Bidder(s) with information to assist in the formulation of their proposals.
3. This RFP does not claim to contain all the information each bidder may require. Each Bidder should conduct its own investigations and analysis and is free to check the accuracy, reliability, and completeness of the information in this RFP and obtain independent advice, wherever necessary. Bank may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.
4. The bank reserves the right to reject any or all Request for Proposals received in response to this RFP document at any stage without assigning any reason whatsoever. The decision of Punjab & Sind Bank shall be final, conclusive, and binding on all the parties.
5. This RFP Document may not be appropriate for all people, and it is not possible for the Bank Representatives, their employees, or advisors to consider the investment objectives, financial situation and particular needs of each party who reads or uses this RFP Document.
6. The Bank, its employees and advisors make no representation or warranty and shall have no liability to any person, including any Applicant or Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form or arising in any way for participation in this bidding process.
7. The provisions of this Agreement shall be governed by the laws of India and the competent court at Delhi shall have exclusive jurisdiction in relation thereto even though other Courts in India may also have similar jurisdictions.

4 INTRODUCTION

Punjab & Sind Bank (hereon referred to as "PSB" or the "Bank"), a body corporate constituted under the Banking Companies (Acquisition and Transfer of Undertakings) Act, 1980, is one of the leading Public Sector Banks in India. The Bank's Corporate Office is located at Kidwai Nagar, New Delhi.

The Bank has a strong nationwide presence through a network of 1,657 branches, 29 Zonal Offices, 74 Head Office Departments, 3 Regional Clearing Centres, and 12 Currency Chests, all operating on a centralized Core Banking Solution (CBS) based on Finacle 10. The Bank also operates a network of more than 1,175 ATMs, including both onsite and offsite ATMs, serving customers across the country. With over 118 years of dedicated customer service, the Bank continues to leverage technology to deliver secure, reliable, and customer-centric banking services.

The Bank has established a centralized Security Operations Centre (SOC) to provide continuous monitoring and management of its IT infrastructure, applications, endpoints, network, cloud, and digital banking ecosystem. The SOC plays a vital role in security event monitoring, threat detection, incident response, cyber threat intelligence, vulnerability management, compliance monitoring, and enhancing the Bank's overall cyber resilience. As the Bank's digital footprint continues to expand and the cyber threat landscape becomes increasingly sophisticated, the SOC is required to evolve into a modern, intelligence-driven, and automation-enabled cybersecurity operations centre capable of delivering proactive threat detection, rapid incident response, and continuous security monitoring.

In line with its cybersecurity strategy and the regulatory guidelines issued by the Reserve Bank of India (RBI), CERT-In, and other applicable authorities & bodies, the Bank intends to further strengthen its cyber defence capabilities through the procurement of the solution mentioned in the RFP.

5 PROJECT OBJECTIVE

The Bank is in the process of upgrading its SOC infrastructure and intends to implement advanced cybersecurity technologies, a NextGEN Security Operations Centre (SOC) solution, and related security applications to safeguard its information assets across the Data Centre in Mumbai, Disaster Recovery (DR) Site in Noida, Cloud Environment, and Bank branches.

This RFP invites technically mature, scalable, and interoperable solutions from eligible bidders to enable the Bank to establish a multi-layered security architecture covering SIEM, SOAR, UEBA, XDR etc.

The bidder shall quote prices strictly in accordance with Appendix 2: Commercial Bill of Material (BoM). The Bank may, if required, procure software, hardware, and services in line with the terms and conditions defined in this RFP, based on the unit rates quoted in the BoM.

The quoted prices shall remain valid for all orders placed during the entire contract period and shall be binding upon the selected bidder.

Interested bidders are required to submit their technical and commercial proposals strictly in the formats prescribed in this RFP document.

The methodology for submission of bids is detailed in Section 6: Instructions to Bidders. The Terms and Conditions (T&C) are provided in Section 14 of this RFP.

This Request for Proposal (RFP) has been prepared solely for the purpose of enabling Punjab & Sind Bank (hereinafter referred to as “the Bank”) to select a bidder for the supply, installation, implementation, maintenance, and management of NextGen SOC & related services.

6 INSTRUCTION TO BIDDER

6.1 Language of the Bid

The bid as well as all correspondence and documents relating to the bid exchanged by the Bidder and the Bank shall be in English language only.

6.2 Bid Currency & Price Structure

Prices shall be expressed in the Indian Rupees only. The cost will not depend on any variation in the dollar exchange rate/change in tax structure. The Total Cost of ownership quoted on GEM should be inclusive of applicable taxes, i.e., GST.

6.3 Bid System Offer

1. The Bid Proposal being submitted would be binding on the Bidder. As such it is necessary that authorized personnel of the firm or organization sign the Bid. The designated personnel should be authorized by a senior official of the Organization having such authority to do so. The same person or a different person should be authorized who should have authority to quote. The Xerox copy of necessary Original Resolutions/ Authority/ Power of Attorney having authority to authorize the person to submit Bid Documents, on behalf of the Company shall be enclosed. The proposal must be accompanied by an undertaking letter duly signed by the designated personnel providing a Bid commitment. The letter should also indicate the complete name and designation of the designated personnel.
2. The bidder shall submit his response to the present tender with the price which will contain the pricing information.
3. Any effort by a Bidder to influence the Bank in evaluation of his bid, bid comparison or contract award decision would result in the rejection of the said bid. The Bank's decision in this case would be final and without prejudice and will be binding on all parties.
4. The Bank reserves the right to accept or not to accept any bid or to reject a particular bid at its sole discretion without assigning any reason whatsoever.
5. The Bids containing erasures or alterations will not be considered. There should be no handwritten material, corrections or alterations in the Bids. All details must be filled in.
6. Bidder staff, personnel and labour will be liable to pay personal income taxes in India in respect of such of their salaries and wages as are chargeable under the laws and regulations for the time being in force, and Bidder shall perform such duties regarding such deductions thereof as may be imposed on him by such laws and regulations.
7. Bidder warrants that it shall be solely liable and responsible for compliance of applicable Labour Laws in respect of its employee, agents, representatives and in particular laws relating to terminal benefits such as pension, gratuity, provident fund, bonus or other benefits to which they may be entitled and the laws relating to contract labour, minimum wages, etc., and the BANK shall have no liability in this regard.

6.4 Two Bid System:

This is two bid system which has the following 2 parts:

Part A- Technical cum Eligibility Proposal: Indicating the response to the Pre-Qualification Criteria, Technical evaluation criteria, Appendix & annexures for Technical and Eligibility requirement, Compliance to Scope of Work and other terms & conditions. The format for submission of Technical Proposal is as per Annexure 1: Submission checklist along with Appendix 1: Functional Compliance Sheet and Appendix 2: Masked Bill of Material.

Part B-Commercial Bid: Furnishing all relevant information as required as per Bill of Material as per Appendix 2.

6.4.1 Preparation for Bids:

6.4.1.1 Part A – Technical cum Eligibility Proposal

1. Before submitting the bid, the bidders should ensure that they have reviewed the terms and conform to the Pre-Qualification Criteria as stated in RFP. Only after satisfying themselves with the Pre-Qualification Criteria, should the Offer be submitted.

2. Technical cum eligibility Proposal should be submitted as per the format in Annexure 1: Submission Checklist. Relevant technical details and documentation should be provided along with Technical Proposal.
3. It is mandatory to provide compliance with the scope, requirements, and terms required by the bank.
4. The offer may not be evaluated and may be rejected by the Bank without any further reference in case of non-adherence to the format or partial submission of information as per the format given in the proposal and not in conformity to the RFP requirement.
5. No modification, alteration, or deviation from the technical and functional requirements proposed by the bidder shall be permitted after submission of the Bid. The submitted proposal shall be treated as final and binding.
6. Bidders shall submit complete details of the proposed solution, including product information, make/brand, model details, product brochures, technical datasheets, functional specifications, and all other relevant supporting documentation along with the Bid. Failure to submit this information along with the offer may result in disqualification.
7. The Technical Proposal shall be complete in all respects and shall contain all information sought under this RFP.

6.4.1.2 Part B - Commercial Bid

1. The Commercial Bid shall be submitted strictly in accordance with the prescribed Bill of Material (BoM), pricing formats, and the terms and conditions specified in this RFP. The Commercial Proposal shall contain complete and accurate pricing information as per Appendix 2. Any deviation from the prescribed BoM structure, modification of the format, omission of pricing information, or failure to submit the Commercial Bid in the prescribed format shall render the Bid liable for rejection.
2. The bidder shall quote its most competitive and final prices in the Commercial Bid. The quoted prices shall be comprehensive and inclusive of all costs associated with the supply, implementation, integration, configuration, testing, commissioning, training, support, maintenance, documentation, licenses, subscriptions, taxes, duties, levies, and any other components required to meet the scope and requirements of the RFP.
3. The Commercial Bid shall be prepared and submitted in a clear, structured, and organized manner, enabling easy evaluation and verification by the Bank. All pricing schedules, line items, quantities, and cost components shall be properly categorized and aligned with the prescribed formats provided in the RFP.
4. The bidder shall ensure that all commercial information furnished in the Commercial Bid is complete, accurate, unambiguous, and consistent with the corresponding Technical Proposal. Any inconsistency, omission, conditional pricing, or ambiguity in the Commercial Bid may result in rejection of the Bid at the sole discretion of the Bank
5. Prices quoted in the Commercial Bid shall remain firm and fixed throughout the validity period of the Bid and for the entire contract period, and shall not be subject to escalation, revision, or adjustment for any reason whatsoever, unless expressly permitted under the terms of the RFP.
6. Any arithmetic errors, discrepancies between unit prices and total prices, or inconsistencies in the Commercial Bid shall be dealt with in accordance with the provisions of the RFP. The Bank reserves the right to seek clarifications or reject the Bid in case of discrepancies.

NOTE:

1. All declarations, claims, certifications, compliances, experience credentials, technical specifications, and other representations made by the bidder in its Bid shall be

supported by appropriate documentary evidence and submitted as part of the Bid. The Bank reserves the right to verify any information, document, or claim furnished by the bidder at any stage of the procurement process.

2. Bidders are advised to carefully examine and fully understand all instructions, eligibility requirements, formats, terms and conditions, scope of work, technical specifications, and other requirements contained in this RFP prior to submission of their Bid.
3. Failure to furnish all information, documents, clarifications, and supporting evidence required under the RFP, or submission of a Bid that is incomplete, inaccurate, misleading, conditional, or not substantially responsive to the requirements of the RFP, shall be solely at the bidder's risk and responsibility and may result in rejection of the Bid without any further reference to the bidder.
4. The Bank shall not be responsible for any omission, misunderstanding, or misinterpretation of the provisions of the RFP by the bidder.

6.5 Cost of Preparation

The bidder shall bear all costs and expenses incurred in connection with the preparation, submission, and participation in the bidding process. The Bank shall not be liable for any such costs under any circumstances, irrespective of the outcome, modification, cancellation, or termination of the bidding process. No claim for reimbursement or compensation shall be entertained by the Bank in this regard.

6.6 Technical Normalization of Bids

The Bank may undertake technical evaluation and normalization of bids for the limited purpose of establishing comparability among technically responsive bids and ensuring that all proposed solutions are evaluated against the common technical and functional requirements specified in this RFP.

Such normalization may include, but shall not be limited to, assessment and alignment of proposed sizing, capacity, deployment architecture (including physical, virtual, cloud, or hybrid models), licensing constructs, and performance requirements as defined in this RFP. The Bank may undertake such evaluations and validation to ensure comparability of bids and suitability of proposed solutions to its operational and technical environment.

Where different OEM architectures, licensing methodologies, deployment models, or sizing approaches are proposed, the Bank may map such proposals to a common requirement baseline for evaluation purposes. Any such normalization shall be carried out uniformly and consistently across all technically responsive bidders and shall not result in any relaxation or modification of the mandatory requirements specified in the RFP.

The Bank may seek clarifications, supporting documentation, sizing calculations, technical assumptions, benchmark reports, and product documentation solely for validation purposes. Such clarifications shall not permit any bidder to alter, revise, enhance, substitute, supplement, or otherwise modify its technical or commercial bid after bid submission.

Where normalization establishes that additional hardware, software, licenses, subscriptions, infrastructure, services, or other components are required to meet the prescribed baseline requirements stated in the RFP, the Bank reserves the right to load the evaluated cost of such components and recompute the evaluated Hardware Cost and/or TCO solely for evaluation purposes and applied consistently and uniformly across all technically responsive bidders to ensure a fair, transparent, objective, and auditable evaluation process.

Such recomputed costs shall be used solely for bid evaluation, TCO calculation, and comparison and shall not affect the bidder's contractual obligations or quoted commercial price.

The Bidders agree that they have no reservation or objection to the normalization process, defined methodology, and all the short-listed bidders will, by responding to this RFP, agree to participate in the normalization process and extend their co-operation to the Bank during this process.

The Bidders, by submitting the response to this RFP, agree to the process and conditions of the normalization process.

6.7 Submission of Bid and communication

The Bank expects the bidders to carefully examine all instructions, terms and conditions mentioned in this RFP document before submitting its unconditional compliance as part of the RFP. Failure to furnish all information required or submission not substantially responsive to the RFP in every respect will be at the bidder's risk and may result in the rejection of Bids.

Bids duly signed and sealed is to be submitted in following form on or before the last Date and Time for bid submission as defined in the Section 1: Key information:

1. The Technical Bid shall be submitted online through the GeM Portal
2. Commercial Bid – Only Online (on GEM Portal)

Any other mode of submission, e.g. by fax, e-mail etc. will not be accepted. No Claim of any Bidder(s) shall be entertained, whatsoever for delayed submission of their bid at any stage because of any reason. Therefore, Bidder (s) are advised to submit their bid well before the scheduled time.

Bids will be opened in the presence of the bidder representatives who choose to attend the opening of tender on the specified date, time and place of bid opening. No separate intimation will be given in this regard.

Bank reserves its right, at its sole discretion to cancel or withdraw the order even after issuing the letter of Intent (LOI) / Purchase Order, if bank receives any directions / orders/ instruction or communication from Statutory Body / RBI/Govt. of India or any other competent authority requiring or directing the bank not to take the project forward or any reasons whatsoever. The decision of the Bank shall be final in this regard without disclosing any reason to any bidder or person.

6.8 Late bids

1. Any bid received after the due date and time for receipts of bids as prescribed in this RFP will be rejected. However, in case of the specified date of submission of bids being declared a holiday for the bank, the bids will be received up to the specified time on the next working day.
2. The bank may, at its discretion, extend this deadline for submission of bids by amending the bid documents, in which case all rights and obligations of the Bank and bidders, previously subject to the deadline, will thereafter be subject to the deadline extended.
3. All such information will be published on Bank's website and https://gem.gov.in/ only. The bidders have to take note of it.

6.9 Modifications and/ or Withdrawal of Bids

1. Bids once submitted will be treated as final and no modification will be permitted. No Correspondence in this regard will be entertained.
2. The Bid should contain no alterations, erasures, or overwriting. The Bidder is expected to examine all instructions, forms, terms and specifications in the bidding documents. Failure to furnish all information required by the bidding documents or submission of

bid not substantially / conclusively responsive to the bidding documents in every respect will be at the Bidders risk and may result in rejection of the bid.

3. No bidder shall be allowed to withdraw the bid after the deadline for submission of bids.
4. In the case of the successful bidder, he will not be allowed to withdraw/back from the bid commitments. The bid earnest money in such eventuality shall be forfeited, and all interests/claims of such bidder shall be deemed as foreclosed

6.10 Earnest Money Deposit (EMD):

1. The bidder shall furnish Noninterest earning Earnest Money Deposit (EMD) amount as mentioned in the Bid Schedule by way of Bank Guarantee drawn on any Scheduled Bank in India (except Cooperative Bank, RRB & Punjab & Sind Bank) in favor of Punjab & Sind Bank, payable at Delhi.
2. The Bidder may also submit the EMD in the form of an Insurance Surety Bond. Refer Annexure 34: Insurance Surety Bond
3. The same should be valid for an additional 45 days beyond bid validity period. Bank at its discretion can demand for extension for the validity of EMD. The format for submission of EMD in the form of Bank Guarantee is as per Annexure 15.
4. The Bank Guarantee issued by the issuing Bank on behalf of Bidder in favor of Bank shall be in paper form as well as issued under the "Structured Financial Messaging System" (SFMS) sent to Punjab & Sind Bank, Sector 44 Branch, Gurgaon, IFSC PSIB0021509. Any bank guarantee submitted in physical mode, including EMD/bid guarantee which cannot be verifiable through SFMS will be rejected summarily.
5. Non submission of EMD leads to rejection of Bid.
6. All MSEs having registration as per provisions of the Public Procurement Policy for Micro and Small Enterprises i.e. District Industries Centre (DIC) or Khadi and Village Industries Commission (KVIC) or Khadi and Industries Board (KVIB) or Coir Board or National Small Industries Commission (NSIC) or directorate of Handicrafts and Handlooms or Udyog Aadhaar Memorandum or any other body specified by Ministry of MSME and Start-ups (recognized by DIPP) are exempted from submission of EMD only. Relevant certificates should be submitted by the bidder in this regard to avail of exemption. Bid Security Declaration should be submitted by eligible MSEs/Startups on Company's letter head with company seal and signature of the authorized person as per Annexure 4.
7. The EMD may be forfeited/ Bank Guarantee may be invoked:
    a) If the bidder withdraws/amends the bid during the period of bid validity (180 days from the date of opening of bid).
    b) If the bidder makes any statement or encloses any form which turns out to be false, incorrect and / or misleading at any time prior to signing of contract and/or conceals or suppresses material information; and / or
    c) The selected bidder withdraws his tender before furnishing the unconditional and irrevocable Performance Bank Guarantee.
    d) The bidder violates any of the provisions of the terms and conditions of this tender specification.
    e) In case of the successful bidder, if the bidder fails:
        i To sign the contract in the form and manner to the satisfaction of Punjab & Sind Bank.
        ii To furnish the Performance Bank Guarantee in the form and manner to the satisfaction of Punjab & Sind Bank.
        iii Bank may proceed against the selected bidder in the event of any evasion, avoidance, refusal or delay on the part of the bidder to sign and execute the

Purchase Order / Service Level Agreements or any other documents, as may be required by the Bank, if the bid is accepted.

iv The Execution of Bid Security Declaration/ Invocation of EMD may suspend participation of the Bidder in any tender in this Bank for three (03) years.

8. Bid securities of the unsuccessful bidders will be returned to them at the earliest after expiry of the final bid validity and latest on or before the 30th day after the award of the contract. The EMD of the selected bidder will be returned within 15 days after submission of Performance Security (PBG) and execution of Contract with the Bank.

6.11 Performance Bank Guarantee (PBG)

1. The successful bidder/s should submit a Performance Guarantee as specified in Key Information **within 30 days from the date of acceptance of Purchase Order**.
2. Performance Guarantee should be submitted by way of Bank Guarantee in favor of Punjab & Sind Bank payable at Delhi / Bank Guarantee may be obtained from any of the Scheduled Commercial Banks (except Cooperative Bank, RRB & Punjab & Sind Bank) for an amount as mentioned in Section 1: KEY INFORMATION.
3. The selected bidder shall be responsible for providing the PBG for the duration of the contract (Including the extension) + claim period (12 months) of the Bank guarantees
4. The Bank Guarantee issued by the issuing Bank on behalf of Bidder in favor of Punjab & Sind Bank shall be in paper form as well as issued under the "Structured Financial Messaging System" (SFMS) sent to Punjab & Sind Bank, Sector 44 Branch, Gurgaon, IFSC PSIB0021509. Any bank guarantee submitted in physical mode, including EMD/bid guarantee which cannot be verifiable through SFMS will be summarily rejected.
5. The PBG applicable must be duly accompanied by a forwarding letter issued by the issuing bank on the printed letterhead of the issuing bank.
6. **Performance Bank Guarantee should be valid for the duration of the contract (Including the extension) + claim period (12 months)**
7. The selected bidder shall be responsible for extending the validity date and claim period of the Bank guarantees as and when it is due, on account of incompletion of the project and contract period.
8. If the Contract is extended, the selected bidder has to submit **fresh PBG for 5% of the extended Contract value and period along with claim period** and also execute fresh/extension of Contract with the Bank **within 15 days from the date of issuance of Purchase Order for renewal.**
9. In the event of the bidder committing a breach of the terms and conditions of the contract, Bank shall provide a cure period of 30 days and thereafter invoke the PBG, if the bidder is unable to service the contract for whatever reason.

6.12 No commitment to accept lowest or any bid

The Bank shall be under no obligation to accept the lowest or any other offer received in response to this tender notice and shall be entitled to reject any or all offers including those received late or incomplete.

The bank reserves the right to make changes in terms and conditions. Bank will be under no obligation to have discussions with any bidder, and/or entertain any representation.

6.13 Right To Accept Any Bid and To Reject Any OR All Bids/ Cancellation of Tender process

Punjab & Sind Bank reserves the right to accept or reject in part or full any or all offers without assigning any reason thereof even after issuance of letter of Intent. Any decision of Punjab & Sind Bank in this regard shall be final, conclusive and binding upon the bidders. The Bank

reserves the right to accept or reject any Bid in part or in full, and to annul the Bidding process and reject all Bids at any time prior to contract award, without thereby incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds for Bank's action. During any stage of evaluation process, if it is found that the bidder does not meet the eligibility criteria or has submitted false /incorrect information the bid will be summarily rejected by the Bank and no further correspondence would be entertained in this regard. The bank reserves the right to amend, rescind, reissue or cancel this RFP and all amendments will be advised to the Bidder, and such amendments will be binding upon them. The Bank also reserves its right to accept, reject or cancel any or all responses to this RFP without assigning any reason whatsoever. Further please note that the bank would be under no obligation to acquire any or all the items proposed. No contractual obligation whatsoever shall arise from the RFP process until and until a formal contract is signed and executed by duly authorized officials of Punjab & Sind Bank and the bidder.

6.14 Correction of Errors

Bidders are advised to exercise greatest care in entering the pricing figures. No corrigendum or requests for prices to be corrected will be entertained after the bids are opened. Discrepancies in bids will be corrected as follows:

1. Where there is a discrepancy between the amounts in figures and in words, the amount in words shall prevail.
2. If there is a discrepancy between percentage and amount, the amount calculated as per the stipulated percentage basis shall prevail
3. Where there is a discrepancy between the unit rate and the line-item total resulting from multiplying the unit rate by the quantity, the unit rate will govern unless, in the opinion of Bank, there is an obvious error such as a misplacement of a decimal point, in which case the line-item total will prevail.
4. Where there is a discrepancy between the amount mentioned in the bid and the line-item total present in the schedule of prices, the amount obtained on totaling the line items in the Bill of Materials will prevail.
5. The amount stated in the correction form, adjusted in accordance with the above procedure, shall be considered as binding, unless it causes the overall price to rise, in which case the bid price shall prevail.
6. In case the bidder does not accept the correction of the errors as stated above, the bid shall be rejected.
7. The Highest Technical bidder shall not automatically qualify for becoming a selected bidder and for award of contract by the bank.
8. The Lowest Commercial Bidder shall not automatically qualify for becoming selected Bidder and for award of contract by the Bank.
9. The commercials will be calculated till two decimal points only. If the third decimal point is greater than .005 the same shall be scaled up else, it shall be scaled down to arrive at two decimal points. Bank will make similar treatment for 4th or subsequent decimal point to finally arrive at two decimal points only.
10. If for some reason, negotiations with the successful bidder fail to result in an agreement within a specified timeline, the Bank reserves the right to award the contract to the next most eligible bidder i.e., the bidder ranked L2, L3 etc. as per the results available on GeM, based on the evaluation.
11. The Bank shall not incur any liability to the affected Bidder on account of such rejection.

Based on the Bank's requirements as listed in this document, the bidder should identify and offer the best-suited solution / bill of material for the product that would meet the Bank's requirements and quote for the same.

During the Tendering process, if any event of conflict arises between the content of the Annexures submitted by bidders and the main body of RFP, then the content of main RFP shall prevail/ applicable.

6.15 Soft copy of tender document

The soft copy of the tender document will be made available on the Bank's website https:// https://gem.gov.in/ , & https://punjabandsind.bank.in/. . However, the Bank shall not be held responsible in any way, for any errors / omissions /mistakes in the downloaded copy.

6.16 Bid validity period

Bids shall remain valid for the period as defined in section 1: Key Information. The Bank holds the right to reject a bid valid for a period shorter than validity period defined in the RFP as non-responsive, without any correspondence. In exceptional circumstances, The Bank may solicit the Bidder's consent to an extension of the validity period. The request and the response thereto shall be made in writing. The extension of validity period by the Bidder should be unconditional and irrevocable. The Bid Security provided should also be suitably extended.

A Bidder acceding to the request will neither be required nor be permitted to modify its bid. A Bidder may refuse the request without forfeiting its bid security. In any case the bid security of the Bidders will be returned after completion of the process.

6.17 Pre-bid meeting

For clarification of doubts of the bidders on issues related to this RFP, the Bank intends to hold a Pre-Bid Meeting on the date and time as indicated in the RFP in Key-Information.

For any clarification with respect to this RFP, the bidder may send an email to soc.tender@psb.bank.in by last date of submission of queries as defined in Key-Information in this document. No queries will be entertained from the bidders after the above date and time.

If the meeting date is declared as a holiday under NI Act by the Government after issuance of RFP, the next working day will be deemed to be the pre-bid meeting day.

The format to be used for seeking clarification is mentioned in Annexure 23 (Pre-bid Query Format). It may be noted that all queries, clarifications, questions etc., relating to this RFP, technical or otherwise, must be in writing only and should be sent to the email-id as stated earlier. No oral or individual consultation will be entertained.

The bank does not have the responsibility to consider any other queries raised by the bidder's representative during the pre-bid meeting.

Participation in the Pre-Bid Meeting shall be restricted to duly authorized representatives of the bidder. The bidder shall submit an authorization letter, duly signed by its authorized signatory, for each representative attending the meeting.

Additionally, the bidder shall share the names, designations, organization details, mobile numbers, and email addresses of the attendees with the Bank at least one (1) working day prior to the date of the Pre-Bid Meeting.

The Bank reserves the right to deny participation to representatives whose details have not been communicated within the stipulated timeline.

The Bank will consolidate all the queries and any further queries during the pre-bid meeting and the replies for the queries shall be made available to all the bidders. The clarification of the Bank in response to the queries raised by the bidder/s, and any other clarification/amendments/corrigendum furnished thereof will become part and parcel of the RFP and it will be binding on the bidders.

The Bank reserves the right not to entertain or respond to any query, clarification request, or representation received after the prescribed deadline for submission of pre-bid queries.

Non-response by the Bank to any query, clarification, or issue raised by a bidder during the Pre-Bid Meeting shall not be deemed as acceptance or concurrence by the Bank. Only responses and clarifications formally communicated by the Bank in writing shall be treated as valid and binding.

6.18 Amendment to RFP Contents

At any time prior to the last date for bid-submission, the Bank may, for any reason, whether at its own initiative or in response to clarification(s) requested by a prospective bidder, modify the RFP contents by Corrigendum. However, it is the bidder's responsibility to keep its communication channels (face-to-face, phone, fax, e-mail etc.) alive including observing Bank's website & GEM Portal for the latest development in this regard. The Bank will not be liable for any communication gap. To provide prospective bidders, reasonable time to take the amendment into account for preparation of their bid, the Bank may, at its discretion, extend the last date for bid-submission.

The bank reserves the right to scrap the tender at any stage without assigning any reason.

6.19 Disqualification

Any form of canvassing/ lobbying/ influence/ query regarding short listing, status etc. will result in disqualification.

6.20 Fixed Price

The prices quoted in the tender response will be fixed for the period of the contract. The price should be exclusive of all taxes and levies which will be paid by the Bank on actual.

6.21 Project Execution

The project shall be executed and completed in a timely and expeditious manner as per the timelines prescribed by the Bank. Upon acceptance of the Purchase Order/Letter of Award, both the Bank and the successful bidder shall nominate a Project Manager who shall serve as the single point of contact for the project. The bidder shall also provide a detailed escalation matrix, including contact details of senior management and key project personnel, to ensure effective project governance and timely resolution of issues. The project manager nominated by the bidder/s should have prior experience in implementing a similar project and meet criteria as defined in RFP

6.22 Confidentiality of the Bid Document

The Bidder, irrespective of his/her participation in the bidding process, shall treat the details of the documents as secret and confidential.

7 SCOPE OF WORK

7.1 Scope and Objectives

The Bank is undertaking a comprehensive enhancement of its Cyber Security and Information Security infrastructure to strengthen its overall security posture across its Data Centre (Mumbai), Disaster Recovery Centre (Noida), Cloud environments, and Branch/Office network. As part of this initiative, the Bank intends to procure, implement, integrate, operate, and maintain advanced Cyber Security technologies, a Next Generation Security Operations Centre (NextGEN SOC), and associated security solutions to safeguard its information assets, critical systems, applications, data, and digital channels against evolving cyber threats.

Through this RFP, the Bank seeks technically robust, scalable, interoperable, and future-ready cybersecurity solutions capable of providing centralized visibility, monitoring, detection, prevention, investigation, response, governance, and compliance across the enterprise. The proposed solution shall establish a comprehensive, multilayered security architecture covering Perimeter Security, Network Security, Endpoint Security, Application Security, Data Security, Cloud Security, Identity Security, AI Security, and Security Compliance Management through a centralized management framework.

The objectives of this procurement are to:

- Achieve end-to-end visibility and centralized management of the Bank's security ecosystem.
- Minimize the attack surface through proactive threat detection, prevention, investigation, and automated response.
- Ensure compliance with RBI guidelines, CERT-In advisories, DPDP Act, Government of India regulations, ISO 27001, and other applicable statutory and regulatory requirements.
- Support the Bank's digital transformation initiatives while maintaining the highest standards of security, resilience, availability, and performance.
- The bank’s architecture requires all external communication to traverse the bank, unless approved by bank.

The proposed solutions shall align with globally accepted cybersecurity frameworks and best practices, including CERT-In Guidelines, NIST Cybersecurity Framework (CSF), MITRE ATT&CK Framework, Zero Trust Architecture (ZTA), and other applicable industry standards. All proposed solutions shall seamlessly integrate with the Bank's existing IT ecosystem and provide centralized management, analytics, reporting, orchestration, and automated response capabilities.

Key Architecture points to be followed:

- All solutions, products, platforms, technologies, and services proposed by the Bidder under this RFP shall be AI-enabled and shall leverage Artificial Intelligence (AI), automation, advanced analytics, or intelligent orchestration to enhance service delivery, operational efficiency, security, automation, and continuous improvement.
- All proposed solutions and services, wherever applicable, shall integrate with the Bank’s Security Information and Event Management (SIEM) platform.
- The Bank’s architecture requires that all communication/traffic shall traverse through the Bank’s designated infrastructure/security controls, unless explicitly approved otherwise by the Bank.
- All SaaS-based proposed solutions shall be designed such that all logs, data, information, scan results, credentials-related metadata, and other security information collected from the Bank's on-premises infrastructure are first collected and processed by the on-premises

scanning component. The on-premises component shall then securely transmit only the required data to the SaaS platform over encrypted communication channels.

- Should have dedicated logical tenant provisioned for bank.
- Customer PII shall not be stored, processed, or transmitted through cloud infrastructure.
- The proposed solution fully secure through Bank-controlled BYOK encryption and exclusive PSB admin authority.
- All the proposed solutions shall support PQC readiness, including support for secure cryptographic mechanisms and standards that facilitate future migration to quantum-resistant cryptography, wherever applicable to the solution. The bidder shall provide the required SSL/TLS certificate for securing data in motion throughout the contract period at no additional cost to the bank.
- All the proposed solutions
    - are the latest commercially available and supported Model(s) and Version(s) offered by the OEM for the relevant product category as on the date of submission of the Bid;
    - are not declared End-of-Sale (EoS) as on the date of submission of the Bid; and
    - shall remain supported by the OEM and shall not reach End-of-Life (EoL) / End-of-Support (EoS) during the Contract Period or for a period of six (6) years from the date of product installation, whichever is later
- OEM architecture should have aggregation at bank's DC & DR through agents/ collectors/ brokers/ aggregators, sensors/ connectors/ scanners, enforcers/ integrators or equivalent components. The SaaS service shall comply with the uptime SLA and other service availability requirements specified in this RFP
- The proposed architecture shall therefore be designed to comply with this requirement

The proposed solution shall support PQC readiness, including support for secure cryptographic mechanisms and standards that facilitate future migration to quantum-resistant cryptography, wherever applicable to the solution. The bidder shall provide the required SSL/TLS certificate for securing data in motion throughout the contract period at no additional cost to the bank.
Considering the Bank's large, complex, and geographically distributed IT infrastructure, the proposed architecture shall be adaptive, distributed, highly available, scalable, and capable of supporting the Bank's current and future security requirements throughout the contract period.
The Disaster Recovery (DR) site shall operate as an active replica of the Primary Data Centre, and all NextGEN SOC components, storage, and infrastructure shall be adequately sized and optimally configured to support future business growth.
The Bidder and respective OEMs shall coordinate with all required third-party vendors and OEMs to ensure seamless interoperability of the proposed solution. Any customization, enhancement, parser development, connector creation, workflow automation, dashboard customization, incident integration, playbook development, reporting customization, alert tuning, remediation activities, APIs, or native integrations required for successful implementation shall be provided without any additional cost to the Bank throughout the contract period.

a. Key Implementation Responsibilities, but not limited to:
    a. The implementation of each proposed solution, including design, installation, configuration, integration, migration, testing, commissioning, user acceptance testing (UAT), and Go-Live, shall be performed by the respective OEM.
    b. The Bidder shall arrange OEM resources, coordinate implementation activities, and ensure timely completion of the project.
    c. Upon successful implementation, the respective OEM shall provide a certificate confirming that the solution has been deployed by the OEM and complies with all functional and technical requirements specified in the RFP and SRS.

b. Key Roles and Responsibilities, but not limited to:
   a. System Integrator (Bidder):
      - Supply all proposed solutions.
      - Manage the overall project.
      - Coordinate with all OEMs and third parties.
      - Provide onsite L1, L2, and L3 support resources.
      - Perform implementation coordination, documentation, knowledge transfer, training, and project governance.

   b. Solution OEM:
      - Design, deploy, integrate, test, commission, configurations/data/logs, optimize performance, and ensure successful implementation of the proposed solution.

c. Security tools, agents, collectors, connectors, sensors, and gateways shall also be deployed within the Bank's Cloud/VPC environments to ensure uniform visibility, monitoring, logging, compliance, and protection across on-premises and cloud infrastructure.

d. The Bidder shall be responsible for implementation, integration, migration, upgrades, patch management, health monitoring, preventive maintenance, troubleshooting, backup and recovery, audit support, documentation, SOP preparation, knowledge transfer, lifecycle management, and operational support for all proposed NextGEN SOC solutions throughout the contract period.

e. All proposed solutions shall support real-time integration, event correlation, orchestration, threat intelligence sharing, automated response, centralized logging, and workflow automation to enable unified security operations.

f. The proposed solutions shall provide configurable dashboards, analytics, executive reports, operational reports, compliance reports, and actionable insights for effective monitoring, governance, and decision-making. Please refer Annexure 25: Indicative List of Reports to be Provided.

g. All proposed solutions, software, appliances, IT infrastructure, operating systems, databases, middleware, application servers, web servers, and all dependent components shall be production-grade, OEM-supported, enterprise-licensed and based on General Availability (GA) releases throughout the contract period.

h. Compliance Requirements

   The proposed solution shall comply with:

   a. The Bank's IT Policy, Information Security Policy, Cyber Security Policy, Cloud Security Policy, Data Governance Policy, Digital Payment Security Controls, and all other internal policies.
   b. RBI Guidelines, CERT-In Directions, Government of India notifications, DPDP Act, NCIIPC, and all applicable regulatory and statutory requirements.
   c. All applicable Indian data protection and privacy laws.
   d. Seamless integration with the Bank's existing on-premises, cloud, and hybrid security ecosystem.

i. General Conditions

   a. If any software, hardware, appliance, subscription, license, or component supplied under this RFP becomes defective, unsupported, reaches End-of-Life (EOL), End-of-Support (EOS), underperforms, or fails to meet the specified functional or performance requirements during the contract period, the Bidder shall replace or upgrade it with an equivalent or higher-capacity OEM-supported component without disruption to Bank operations and without additional cost.
   b. The Bidder shall take all necessary corrective measures to rectify any defect, degradation, incompatibility, or performance issue affecting the proposed solution within the agreed SLA and without additional cost to the Bank.

c. The proposed solution shall include all software licenses, subscriptions, hardware, appliances, accessories, operating systems, databases, middleware, APIs, connectors, utilities, infrastructure components, and all associated dependencies necessary for successful installation, integration, commissioning, operation, maintenance, scalability, security, and support.

d. Any software, hardware, services, licenses, utilities, accessories, connectors, APIs, middleware, operating systems, databases, or other components not explicitly mentioned in this RFP but required for successful implementation, operation, performance, security, integration, scalability, availability, or completeness of the proposed solution shall be supplied by the Bidder without any additional cost to the Bank.

e. The Bidder shall remain solely responsible for any assumptions, omissions, sizing errors, technical discrepancies, incompatibilities, or design deficiencies in its proposal irrespective of any review, acceptance, or approval by the Bank.

f. The successful Bidder shall provide end-to-end services covering design, supply, implementation, integration, migration, testing, commissioning, training, documentation, OEM coordination, monitoring, operations, maintenance, warranty, post-warranty support, audit support, upgrades, lifecycle management, and technical support throughout the contract period. The Bidder shall remain fully responsible for the availability, security, performance, functionality, and support of the complete solution without any additional cost to the Bank.

7.1.1 RACI Matrix

Sl. No.	Activity / Deliverable	Bank	Bidder	OEM	CSP (Where Applicable)
1	Requirement Gathering & Analysis	C	A	R	I
2	Assessment of Existing Environment	C	A	R	I
3	Functional & Technical Design Documentation	A	R	R	I
4	Solution Architecture & Design	C	A	R	C
5	Solution Sizing & Capacity Planning	I	A	R	C
6	Installation, Configuration & Customization	I	A	R	I
7	Integration with Existing Systems	C	A	R	C
8	Development/Configuration of APIs, Connectors & Interfaces	I	A	R	C
9	Implementation of Security Controls	C	A	R	C
10	High Availability & Disaster Recovery Implementation	C	A	R	C
11	Testing (Functional, Integration, Performance & Security)	C	A	R	I
12	User Acceptance Testing (UAT) Support	A	R	R	I
13	Defect Resolution & Remediation	I	A	R	C
14	Go-Live Planning & Production Deployment	C	A	R	C
15	Documentation & Knowledge Transfer	C	A	R	I
16	Training & Certification	I	A	R	I
17	Health Checks, Reviews & Performance Optimization	I	A	R	C
18	Patch Management, Upgrades & Technology Refresh	I	A	C	C
19	Policy, Rule & Configuration Tuning	I	A	C/R	I
20	Incident, Problem & Change Management Support	C	A	C	C
21	Project Governance, Reporting & Reviews	A	R	C	I
22	Risk Management & Escalation	C	A	C	I

Sl. No.	Activity / Deliverable	Bank	Bidder	OEM	CSP (Where Applicable)
23	Backup, Recovery & Business Continuity Support	C	A	C	C
24	Exit Management, Transition & Knowledge Handover	C	A/R	C	C/I

7.2 Solution & Services Deployment Model and Their HA Requirement

7.2.1 Solutions – Master Deployment Matrix

Refer Annexure 21 of the RFP for the updated Section

7.2.2 Services

Refer Annexure 21 for the updated Section

.

7.2.3 Deployment Model Definition

Refer Annexure 21 of the RFP for the updated Section

7.2.4 Deployment Architecture

Refer Annexure 21 of the RFP for the updated Section

7.3 Functional Requirements - Solutions

7.3.1 Security Information and Event Management

As part of the SIEM solution implementation, the bank expects the system to meet the requirements of a Next-Generation Security Operations Centre (SOC) enhanced with AI/ML capabilities (e.g., anomaly detection, false positive reduction, behavior analytics, risk based prioritization and threat prediction.

SIEM should be major driving engine in the NextGen SOC. Entire IT Infrastructure of the Bank and other IT security & NextGen SOC systems & services should be integrated with SIEM.

SIEM should withstand extremely high IOPS at collection, correlation, analytics & alerting layers and provide intelligent and interactive dashboards with deep-dive analytical and visualization capabilities.

As a part of the deployment bidder to consider that logs shall be collected from a wide range of sources across the bank's IT environment both on-premises as well as on-cloud (public & private). Sources should include (existing and new/future) not limited to:

- Entire IT infrastructure
- All Network Devices
- All IT security solutions
- All Applications
- All NextGEN SOC technologies

7.3.1.1 Modules, Architecture & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: SIEM.
2. Support a modular, distributed, scalable, fault-tolerant, and enterprise-grade architecture capable of accommodating the Bank's current and future growth without service disruption.
3. Integrate with the Bank's entire IT ecosystem, including on-premises, cloud, hybrid, legacy, and future infrastructure.

4. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.
5. Support integration with all proposed NextGEN SOC solutions, including SOAR, UEBA, XDR, TIP, CSPM, CNAPP, CWPP, CTEM, ITDR, Application Security Testing (AST), Deception Technology, Vulnerability assessment (VA) & vulnerability lifecycle management security services, and other security solutions, details of which shall be provided to successful bidder.
6. Support collection of logs and telemetry from, at a minimum:
   a) Servers (Physical & Virtual)
   b) Endpoints
   c) Network Devices
   d) Security Appliances
   e) Databases
   f) Applications
   g) Access Management solutions
   h) Cloud Platforms (Public & Private)
   i) SaaS, PaaS and IaaS Services
   j) Containers and Kubernetes
   k) APIs and Microservices
   l) Third-party systems and services
7. All SIEM components, including collectors, ingestion nodes, correlation engines, processing nodes, etc., are deployed in the prescribed HA architecture irrespective of whether they are deployed at the Bank's Data Centre (DC), Disaster Recovery (DR) Centre, CSP Primary Site, or CSP Secondary Site.
8. Where a SIEM Broker, Data Pipeline, Collector, Gateway or similar component is proposed for filtering, aggregation, deduplication, suppression or routing of events prior to SIEM ingestion, the Bidder/OEM shall provide visibility of the input EPS, processed EPS, filtered/suppressed/aggregated events and final EPS forwarded to the SIEM. Any claimed data-reduction ratio shall be demonstrable and auditable.
9. The solution shall support the creation, modification, historical testing, and tuning of customized detection and correlation rules by authorized SOC personnel.
10. The solution shall provide rule-level statistics including alerts generated, true positives, false positives, and rules with no events.
11. The solution, or its natively integrated Threat Intelligence Platform (TIP), shall support industry-standard threat-intelligence exchange mechanisms including STIX/TAXII or equivalent.
12. The solution shall provide AI-assisted incident summarization, investigation, root-cause analysis, threat hunting, query generation, and recommended investigation steps.
13. AI-generated detections shall provide supporting evidence and context from underlying security events and allow analyst validation as True or False Positives.
14. The solution shall maintain an audit trail of executed queries and associated analyst actions.
15. The SIEM shall use AI/ML to automatically correlate and triage security alerts by reducing false positives, prioritizing alerts based on risk, summarizing relevant context and evidence, and recommending investigation and response actions, with full explainability and auditability.
16. The solution shall support detection/correlation of unauthorized AI service usage, abnormal AI/API activity, compromise or misuse of AI infrastructure, AI-related data exposure/leakage and AI-enabled malicious activities, based on available telemetry.
17. The solution shall integrate with DLP, Identity, Cloud, API, and Application Security solutions for correlation and investigation of threats.

18. The solution shall display the status/outcome of SOAR actions and maintain correlation between the originating alert/incident and corresponding response action.
19. The solution shall provide granular RBAC with integration with enterprise SSO/MFA and support segregation of access based on user roles and administrative privileges.
20. Key administrative and security-sensitive activities, including user access changes and configuration updates, shall be auditable.
21. All ingested customer logs and data shall remain the property of the Bank throughout the contract period and upon expiry/termination.

7.3.1.2 SIEM Data Ingestion and EPS Measurement

The proposed solution shall support SIEM sizing based on actual data ingested by the SIEM, measured in Events Per Second (EPS) and/or Daily Data Ingestion (GB/day or TB/day), as applicable.

SIEM EPS shall mean the number of unique log records/events actually delivered to and ingested by the SIEM for SIEM processing.

EPS shall be measured at the SIEM ingestion boundary, after applicable source-side filtering or selection and at or immediately before the SIEM processing boundary.

Each unique event/log record shall be counted only once for SIEM EPS. Internal telemetry, intermediate processing records, replicated records, correlated alerts, or downstream workflow events shall not be counted as additional SIEM source-ingestion EPS unless they are separately generated as unique records and actually ingested by the SIEM.

Where XDR (or any other solution) and SIEM are provided by the same OEM, including where they utilize a common data platform, shared cloud backend, the Bidder shall clearly identify and distinguish:

- XDR (or any other solution) native telemetry;
- Data actually ingested and processed by the SIEM;
- SIEM-generated or correlated events; and
- Data exchanged between the XDR (or any other solution) and SIEM platforms.

The use of common OEM architecture or shared backend shall not be used to combine or double-count data volumes for SIEM EPS calculation. XDR (or any other solution) native telemetry shall not be treated as additional SIEM EPS where it is not separately ingested by the SIEM for SIEM processing.

The Bidder shall clearly state the proposed EPS and corresponding daily data ingestion capacity (GB/day or TB/day), along with the applicable measurement methodology and assumptions, as part of the technical response.

For solutions where XDR (or any other solution) and SIEM capabilities are delivered through a unified security platform, the Bidder shall demonstrate how the proposed architecture avoids duplicate ingestion, duplicate storage, and artificial inflation of SIEM EPS while maintaining the required security analytics and detection capabilities.

7.3.1.3 Key Deliverables:

1. The service delivery (SLA Management) and periodic reporting through automated dashboards.

2. Log Baselining & Log Source health monitoring
3. Creation/customization of parser for unknown/customized log sources
4. Creation, tuning and maintenance of detection/correlation Rules and policies
5. Advanced query capabilities for threat hunting, investigation and detection engineering.
6. AI/ML-assisted security analytics, investigation, threat detection, prioritization and response capabilities.
7. The solution shall provide a consolidated Enterprise SOC dashboard providing an integrated view of SIEM, XDR, SOAR, UEBA, threat intelligence, and other relevant cybersecurity components.
8. Role-based dashboards for Top Management, Department Heads, CISO, System Administrator, Network/Security Administrator, Application Administrator and Auditor.
9. Reports covering:

    a. Total alerts/rules triggered
    b. True Positive vs False Positive
    c. MITRE ATT&CK coverage and gaps
    d. Rules with no events
    e. Log-source health
    f. Detection effectiveness
    g. Incident volume/severity
    h. MTTA/MTTR
    i. SLA compliance
    j. Threat-intelligence
    k. AI-related security events/incidents
    l. Detection and response trends

7.3.2 SOAR (Security Orchestration, Automation, & Response)

The bank requires a solution that can efficiently manage and respond to security incidents while ensuring regulatory compliance. A SOAR platform can automate the incident response lifecycle, from detecting security threats to executing predefined actions for containment, remediation, and recovery enabling bank to optimize its security operations, improve incident management, and ensure a faster, more effective response to cyber threats.

7.3.2.1 Modules, Architecture & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: SOAR.
2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.
3. The solution shall support investigation and response workflows for security incidents involving applications, platforms and APIs, including unauthorized usage, data exposure/leakage, abnormal API activity and compromise or misuse of services, based on available telemetry.

7.3.2.2 Key Deliverables

1. Implementation and configuration of security orchestration and automated response capabilities.
2. Integration with SIEM, XDR, UEBA, TIP, ITSM, IAM/PAM, network, endpoint, cloud and other relevant security solutions.
3. Development, customization, testing, tuning and maintenance of response workflows, playbooks and organization-specific use cases.
4. Implementation of automated alert enrichment, investigation, containment, remediation and response-verification processes, with appropriate approval and exception controls.

5. AI/ML-based capabilities for security investigation, prioritization and response, where applicable.
6. Dashboards and reports covering incidents, response activities, automation, SLA, MTTA, MTTR and response effectiveness.
7. Backup, retention, restoration, documentation and knowledge transfer for configured security automation capabilities and use cases.

7.3.3 UEBA (User and Entity Behavior Analytics)

The Bank requires a solution that provides the ability to continuously monitor and analyze user and entity behaviors across the network. Solution should detect anomalies such as unusual login times, abnormal data access patterns, or suspicious file transfers that deviate from established baselines of normal behavior.

UEBA should provide quick, accurate, efficient and complete replay of attack / kill chain life cycle on the console and reports right from reconnaissance, external penetration, gaining a foothold, deliver payload, appropriating privileges, lateral movement, internal reconnaissance, data collection, maintain presence & exfiltration of data, information, logs, self-destruct, wipe out forensic proof etc.

UEBA should withstand extremely high IOPS at collection, correlation & alerting layers.

Entire IT infrastructure of the Bank must be integrated with the UEBA for the purpose.

The solution would be required to monitor behavior patterns, create a detailed audit trail, documenting each action taken by users within the system.

7.3.3.1 Modules, Architecture & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: UEBA.
2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.
3. Detect/investigate anomalous behaviour associated with applications and APIs, based on available telemetry.
4. Visibility into generated behavioural anomalies, assigned risk scores, and the underlying events that triggered the risk-scoring logic.

7.3.3.2 Key Deliverables:

1. SOPs and relevant UEBA operational documentation.
2. Configured behavioural baselines for users and entities.
3. Configured peer groups, trusted entities and relevant behavioural-analysis parameters.
4. Configured and tuned behavioural analytics and detection use cases.
5. Configured risk scoring and anomaly thresholds.
6. Configured dashboards and reports.
7. Integration with SIEM, SOAR and other required security solutions.
8. Periodic tuning, false-positive reduction and optimization of behavioural analytics and detections.
9. Configured automated response workflows for approved high-risk behavioural alerts.
10. Reports covering user/entity risk, anomalies, behavioural trends, privileged-user activities, attack activities and detection effectiveness.

7.3.4 Extended Detection and Response (XDR)

The Bank requires the solution to provide comprehensive Extended Detection and Response (XDR) capabilities across endpoints and servers. The solution shall provide continuous endpoint visibility, telemetry collection, threat detection, behavioural analysis, investigation, threat hunting, endpoint forensics and response capabilities. The solution shall support

detection and response against advanced threats including ransomware, fileless malware, zero-day and other sophisticated attacks.

The XDR solution shall support integration with the Bank's existing endpoint security environment, SIEM, SOAR, UEBA, ITSM and other relevant security solutions, as applicable.

7.3.4.1 Modules, Architecture & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: XDR
2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.

7.3.4.2 Key Deliverables:

1. Threat detection and response reports covering:
   a. Advanced endpoint threat detection
   b. Endpoint correlation analytics and security insights
   c. Automated and manual response actions
   d. Threat hunting outcomes
   e. Endpoint forensic investigation and analysis
2. SOPs and relevant XDR operational documentation.
3. Configured custom dashboards and reports.
4. Configured and tuned endpoint detection and behavioural analytics.
5. Configured endpoint, user and entity baselines, where applicable.
6. Configured integrations with SIEM, SOAR, UEBA, XDR and other required security solutions.
7. Periodic tuning, false-positive reduction and optimization of endpoint detections.

7.3.5 Network detection and response (NDR)

The **Network Detection and Response (NDR) requirement has been deleted**. Accordingly, the corresponding capabilities should be demonstrated through the proposed XDR platform, refer revised XDR specification.

7.3.6 Decoy/HoneyPOT

A Decoy/HoneyPot solution should act as a decoy system that mimics sensitive financial systems, enticing attackers to engage with fake assets instead of real ones. This allows security teams to monitor attack patterns and behaviour without compromising actual banking infrastructure providing bank a unique opportunity to collect threat intelligence that can be used to reinforce security environment.

7.3.6.1 Modules, Architecture & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: Decoy/ HoneyPot.
2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.

7.3.6.2 Key Deliverables:

1. The bidder should Provide a Centralized Management Console with customizable dashboard and role-based admin.

2. Restore the logs/data from backup for forensic investigation and as per bank requirement without any additional cost.

7.3.7 Threat Intelligence Platform

Bank requires a specialized solution designed to aggregate, analyze, and share cyber threat data and intelligence from multiple sources to help bank detect, understand, and respond to potential security threats. The platform serves as a central hub for collecting, enriching, and distributing information about emerging threats, attack trends, and tactics used by cyber adversaries.

7.3.7.1 Modules, Architecture & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: Threat Intelligence Platform.
2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.
3. The solution shall automatically aggregate and normalize threat intelligence received from multiple sources while retaining source and relevant contextual information.
4. The solution shall maintain intelligence metadata including, as applicable, source, confidence, first-seen, last-seen, and expiration information.
5. The solution shall support threat-intelligence scoring and prioritization based on source reliability, confidence, severity, and other applicable attributes
6. The solution shall support matching and contextualization of threat intelligence against available security telemetry and assets to determine relevance and potential impact to the Bank
7. The solution shall natively leverage validated threat intelligence within its automation and response workflows to facilitate response actions.
8. The solution shall provide IOC lifecycle management, including creation, validation, enrichment, scoring, distribution, updating, and expiration of indicators.
9. The solution shall support configurable expiry periods for indicators based on indicator type, feed source, or global retention policies.
10. The solution shall support threat-intelligence lifecycle workflows for validation, enrichment, curation and dissemination of intelligence.

7.3.7.2 Key Deliverables:

1. Implementation and configuration of threat-intelligence capabilities and required integrations.
2. Configuration of threat-intelligence collection, normalization, enrichment, validation, scoring and dissemination.
3. Management of indicator lifecycle, including IOCs, IOAs and TTPs.
4. Integration with SIEM, SOAR, XDR, UEBA, CTEM, vulnerability management and other relevant security solutions.
5. Configuration of threat-intelligence use cases, alerts, dashboards and reports.
6. Threat-intelligence reports covering:
   a) Malware and vulnerability analysis
   b) Threat actors and advanced threats
   c) Security news, trends and forecasts
   d) Country and industry risk
   e) Vulnerability exploitation tracking
   f) IOCs, IOAs and TTPs
   g) Crimeware and ransomware

h) State-sponsored and other threat actors
i) Emerging technology threats

7. Custom threat-intelligence reports for significant security incidents and regulatory requirements.
8. Periodic review, tuning and optimization of threat-intelligence sources, analytics and use cases.
9. SOPs, documentation and knowledge transfer.
10. Retrieval and restoration of historical threat-intelligence data for investigation and forensic requirements.

7.3.8 Vulnerability assessment (VA) & vulnerability lifecycle management

The Vulnerability Assessment (VA) and vulnerability lifecycle management solution shall enable the Bank to proactively protect its infrastructure, applications, identities, and digital assets by continuously identifying vulnerabilities, detecting identity-based threats, and monitoring suspicious activities across hardware, software, network, cloud, endpoint, and authentication environments before they can be exploited by attackers.

The proposed solution shall support both automated and manual methods to identify security weaknesses and anomalous identity activities.

7.3.8.1 Modules, Architecture & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: VA Tool.
2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.

7.3.8.2 Key Deliverables:

1. Vulnerability reports and dashboards.
2. Asset discovery and onboarding.
3. Authenticated and unauthenticated vulnerability assessments.
4. Vulnerability prioritization and remediation management.
5. Vulnerability lifecycle management.
6. Integration with ITSM, CMDB, threat intelligence and other relevant systems.
7. Vulnerability exception and accepted-risk management.
8. Periodic assessment, re-assessment and remediation validation.
9. SOPs, documentation and knowledge transfer.
10. Retrieval and restoration of required vulnerability data for investigation and Bank requirements

7.3.9 Identity Threat Detection & response

The proposed Identity Threat Detection & Response (ITDR) solution shall enable the Bank to continuously monitor, detect, investigate, prioritize, and respond to identity-related security threats and anomalous activities across user identities, privileged identities, service accounts, application identities, administrative accounts, and other relevant entities.

The solution shall identify and respond to identity-based threats, including compromised credentials, anomalous authentication activities, privilege misuse, unauthorized access, suspicious account behaviour, privilege escalation, lateral movement involving identities, credential abuse, and other identity-related security risks. The solution shall support automated, semi-automated, and manual methods for identity threat detection, investigation, and response.

7.3.9.1 Modules, Architecture & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: ITDR Tool.
2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.
3. The solution shall support integration with relevant identity sources, including Active Directory, Entra ID, LDAP, IAM, SSO, cloud identity providers and other Bank-approved identity repositories, as applicable. The solution shall detect suspicious authentication activities, including unusual authentication patterns, abnormal authentication locations, impossible travel, unusual access times and repeated authentication failures, where applicable telemetry is available.
4. The solution shall support identity-threat investigation and case management, including evidence, investigation activities, response actions, status, ownership and outcome.
5. The solution shall support customizable identity-threat detection queries and policies based on Bank-defined requirements
6. The solution shall support identity-specific response actions, including account disablement, session termination, credential reset, access revocation and privilege removal, where supported by the integrated identity controls.
7. The solution shall display the outcome of identity response actions directly within the associated identity incident.
8. The solution shall support configurable alerting, escalation and notification for high-risk identity threats, compromised identities and Bank-defined identity-security conditions.
9. The solution shall maintain an audit trail of identity-threat investigation, response actions, and outcomes.
10. The solution shall provide dashboards and reports covering key identity metrics, including suspicious authentication, identity threats, lateral movement, and incident status, with support for customizable reporting.
11. The solution shall support cloud and hybrid identity environments, including relevant non-human/application identities, wherever applicable.
12. The solution shall support AI/ML-assisted identity-threat detection and risk prioritization using available identity, authentication, privilege and access context, with the ability for authorized personnel to review and validate identified threats.

7.3.9.2 Key Deliverables:

1. Implementation and configuration of identity threat detection and response capabilities.
2. Integration with relevant identity sources and security solutions.
3. Configuration of identity-threat detection, risk scoring and prioritization.
4. Configuration of identity-threat investigation and response workflows.
5. Identity-threat dashboards, alerts and reports covering identity risks, suspicious authentication, credential abuse, privilege misuse, lateral movement and related threats.
6. Periodic tuning and optimization of detection and risk analytics.
7. SOPs, documentation and knowledge transfer.
8. Retention, backup, retrieval and restoration of required ITDR data and reports for investigation and forensic requirements, without additional cost.

7.3.10 Application security testing Tool

The Bank is looking to enforce application security testing from the early stage of development, with that as a goal the Bank has decided to implement SAST & DAST Solution for analyzing web applications, Mobile Applications & APIs.

7.3.10.1 Modules, Architecture & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: AST.
2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.
3. The solution shall identify application security vulnerabilities including insecure third-party components/dependencies, sensitive-data exposure, infrastructure-as-code misconfigurations, and runtime web/API threats.
4. The solution shall support application security scanning and assessment based on recognized application-security standards and classifications, including OWASP and CWE, as applicable
5. The solution shall support security assessment of container images and associated software components, including identification of known vulnerabilities, outdated or unsupported components, insecure configurations and other applicable security risks. The solution shall support scanning of container images from supported repositories/registries and integration with applicable CI/CD workflows.
6. The solution shall support contextual risk prioritization of application security findings using factors including vulnerability severity, exploitability, likelihood, application criticality, deployment environment, exposure and other relevant contextual factors. Risk-prioritization parameters shall be configurable by authorized users.
7. The solution shall support configurable security policies/security gates for identifying applications or builds that do not meet Bank-defined application security criteria.

7.3.10.2 Key Deliverables:

1. SAST, DAST, API, Mobile Security and SCA implementation and configuration.
2. Application, API, mobile application and code repository onboarding.
3. CI/CD and DevSecOps integration.
4. Security policies, rules and security gates configuration.
5. Vulnerability assessment, validation and re-testing.
6. Dashboards, reports and required compliance artefacts.
7. Periodic assessment, tuning and re-validation.
8. SOPs, documentation and knowledge transfer.
9. Data retention, backup, retrieval and restoration as per Bank requirements.
10. Ensure that the reports are extracted from online / warehouse storage etc. Restore the logs/data from backup for forensic investigation and as per bank requirement without any additional cost.

7.3.11 Cloud Security (CSPM) Tool

Bank is embarking on its cloud transformation journey and intends to establish a robust and comprehensive cloud security posture across all cloud environments. The Bank's objective is to implement an integrated Cloud security solution that provides a centralized and unified single-pane-of-glass view across all cloud assets, workloads, identities, configurations, applications, containers, AI services, and cloud-native resources deployed across multi-cloud, hybrid-cloud, and on-premises environments.

By continuously aligning cloud configurations with industry benchmarks and internal policies, the tool is required to play a key role in reducing the attack surface and supporting regulatory compliance efforts.
The proposed solution shall include all required licenses, subscriptions, connectors, agents, modules, and functionalities:

7.3.11.1 Modules, Architecture & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: CSPM.
2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.
3. The solution shall assess applicable cloud security-control configurations, including logging, monitoring, encryption and other Bank-defined security controls.
4. The solution shall detect configuration drift from approved security baselines and Bank-defined policies.
5. The solution shall identify unresolved and recurring cloud-security posture findings following subsequent assessments.
6. The solution shall support exception/accepted-risk management for cloud-security posture findings, including justification, approval, ownership, validity period and review/expiry.
7. The solution shall provide alerts/notifications for critical/high-risk cloud-security posture findings and Bank-defined policy violations.
8. The solution shall maintain historical information on cloud-security posture findings to support tracking of open, remediated, and recurring findings.
9. The solution shall provide dashboards and reports covering key cloud-security metrics, including overall security posture, critical misconfigurations, exposed resources, accepted risks, and compliance trends, with support for customizable reporting.
10. The solution shall support machine-readable and human-readable export of cloud-security posture findings and compliance information for authorized stakeholders and systems.
11. The solution shall support integration with ITSM/CMDB and other Bank-approved systems for assignment and tracking of cloud-security posture findings and remediation status.

7.3.11.2 Key Deliverables:

1. Solution Architecture Document
2. Cloud Asset Discovery & Inventory Report
3. Configuration & Policy Setup
4. Misconfiguration Assessment Report
5. Risk Prioritization & Remediation Tracking.
6. Configuration Drift & Exposure Monitoring.
7. Remediation Validation & Exception Management.
8. Integration with Cloud APIs, ITSM/CMDB and other relevant systems.
9. SOPs, Documentation & Knowledge Transfer.
10. Incident Response & Automated Playbooks
11. Reporting, dashboards, and capabilities to provide adequate artefacts and reports for executive as well as management to meet ops and regulatory compliance requirements.

7.3.12 Cloud-Native Application Protection Platform (CNAPP)

The Bank intends to implement a Cloud-Native Application Protection Platform (CNAPP) to provide centralized visibility, continuous risk assessment, and integrated protection for cloud-native applications throughout their lifecycle across multi-cloud, hybrid-cloud, and on-premises environments.

The proposed CNAPP shall provide a unified security platform to identify, prioritize, correlate, and remediate risks across cloud applications, identities, Infrastructure-as-Code (IaC), APIs, containers, Kubernetes environments, and other cloud-native resources. The solution shall consolidate security findings from various cloud security domains to provide contextual risk analysis, attack path visualization, and prioritized remediation recommendations.

The proposed solution shall include all required licenses, subscriptions, connectors, agents, modules, APIs, and functionalities required to deliver the complete scope of work without requiring any additional third-party components unless specifically proposed by the Bidder.

7.3.12.1 Modules, Architecture & Deployment:

1. Proposed solution shall comply with the requirements specified in Appendix-1: Functional Compliance Sheet (CNAPP)
2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.
3. The solution shall support software composition analysis (SCA), Infrastructure-as-Code (IaC) scanning, and secrets scanning for frameworks used by cloud-native applications.
4. The solution shall correlate API security findings with associated applications, cloud resources, workloads, identities and network resources to provide contextual cloud-native risk.
5. The solution shall support identification of security risks introduced through changes to IaC, application configurations and deployment environments.
6. The solution shall support configurable cloud-native security policies and security gates for applicable development and deployment processes.

7.3.12.2 Key Deliverables:

1. Solution Architecture Document.
2. Cloud Application Discovery & Inventory Report.
3. Source-Code Security Assessment Report.
4. Software Composition Analysis (SCA) Report
5. Container & Kubernetes Security Assessment Report.
6. Infrastructure-as-Code (IaC) Security Configuration & Assessment Report.
7. Identity & Entitlement Risk Assessment Report.
8. API Security Assessment Report.
9. Cloud Attack Path Analysis Report.
10. CI/CD & DevSecOps Integration.
11. Security Policy & Security Gate Configuration.
12. Remediation Validation & Re-assessment Report.
13. Cloud Risk Prioritization & Remediation Report.
14. Executive Dashboards, Operational Dashboards, and Regulatory Compliance Reports.
15. Configuration of security policies, integrations, connectors, dashboards, and reporting.
16. Restoration of configuration data, audit logs, reports, and operational data from backup for audit, forensic investigation, and regulatory requirements without additional cost to the Bank.

7.3.13 Cloud Workload Protection Platform (CWPP)

The Bank intends to implement a Cloud Workload Protection Platform (CWPP) to provide comprehensive security for cloud workloads deployed across public cloud, private cloud, hybrid cloud, and on-premises environments.

The proposed solution should provide centralized visibility, continuous monitoring, vulnerability assessment, runtime protection, threat detection, workload integrity monitoring, malware protection, configuration assessment, and security policy enforcement for virtual machines, containers, Kubernetes clusters, serverless workloads, and cloud-native compute resources throughout their lifecycle.

The proposed solution shall include all required licenses, subscriptions, connectors, agents, sensors, modules, APIs, and functionalities necessary to provide complete workload protection without requiring any additional third-party components unless specifically proposed by the Bidder:

7.3.13.1 Modules, Architecture & Deployment:

1. Proposed solution shall comply with the requirements specified in Appendix-1: Functional Compliance Sheet (CWPP).
2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.
3. The solution shall support vulnerability assessment of supported cloud workloads, including operating systems, installed software, packages and applicable workload components.
4. The solution shall identify known vulnerabilities in supported workload operating systems, software packages and components and provide associated severity/risk information.
5. The solution shall support vulnerability assessment of container images, including identification of vulnerable packages and components, where applicable.
6. The solution shall correlate identified workload vulnerabilities with the affected workload, component, severity and runtime context to support risk prioritization.
7. The solution shall maintain historical information on open, remediate and recurring workload vulnerabilities.
8. The solution shall support detection of container-runtime security threats, including container escape attempts, where technically supported.
9. The solution shall support configurable workload protection policies, rules and thresholds.
10. The solution shall provide workload-specific risk/severity classification and prioritization of vulnerability and run-time-security findings.
11. The solution shall maintain historical information on runtime threats, malware detections, integrity violations, vulnerabilities and protection actions.
12. The solution should provide dashboards and reports covering key workload-security metrics, including workload vulnerabilities, runtime threats, file-integrity violations, container/Kubernetes threats, and protection actions, with support for customizable reporting.
13. The solution shall maintain an audit trail of workload-security detections, policy changes, and protection actions.
14. The solution shall support integration with SIEM, SOAR, XDR and other Bank-approved security systems for exchange of workload-security alerts and information.

7.3.13.2 Key Deliverables:

1. Solution Architecture Document.
2. Cloud Workload Discovery & Inventory Report.

3. Workload Protection Policy Configuration Report.
4. Vulnerability Assessment Report for Cloud Workloads.
5. Runtime Threat Detection & Protection Configuration Report.
6. Container & Kubernetes Security Assessment Report.
7. File Integrity Monitoring & Malware Protection Configuration Report.
8. Workload Vulnerability Remediation, Network Security, Isolation/Containment and Serverless Security Assessment Report, where applicable.
9. Workload Security Audit Trail and Protection Activity Report.
10. Executive Dashboards, Operational Dashboards, and Regulatory Compliance Reports.
11. Configuration of workload protection policies, connectors, integrations, dashboards, and reporting.
12. Restoration of configuration data, audit logs, reports, and operational data from backup for audit, forensic investigation, and regulatory requirements without additional cost to the Bank.

7.3.14 Continuous Threat Exposure Management (CTEM) Tool

The bank intends to establish a continuous Threat Exposure Management (CTEM) for comprehensive threat exposure management and vulnerability management program integrating all the necessary tools and services including Vulnerability Management (VM) and Breach and Attack Simulation (BAS). The objective is to shift the from reactive, point-in-time scanning centric approach to a more comprehensive, contextual rich, proactive risk-based threat management.

The Bidder shall leverage all the required services and technologies to provide an integrated, unified 'Risk Dashboard' that operationalizes the 5 stages of the CTEM framework (Scoping, Discovery, Prioritization, Validation, and Mobilization). This dashboard must provide a single-pane-of-glass view that correlates technical vulnerabilities (VM) with simulated attack paths (BAS), allowing the Bank to visualize the real-world exploitability of its assets.

The Bidder is required to propose supplementary tools, orchestration layers, or managed services to ensure the full CTEM framework expectations are met without exception.

7.3.14.1 Modules, Architecture & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: CTEM.
2. - The proposed solution should have Two-Factor Authentication (2FA) and as an when bank brings its own MFA then solution should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.
3. The solution shall support creation and management of CTEM scopes based on business units, applications, assets, asset groups, environments, technologies, locations, business criticality and other Bank-defined criteria.
4. The solution shall support identification of business-critical assets and attack surfaces within defined CTEM scopes.
5. The solution shall support association of business criticality and relevant business context with assets and exposures for risk assessment.
6. The solution shall support re-validation of exposures after remediation or security-control changes.
7. The solution shall maintain historical records of validation activities, validation results and exposure-status changes.
8. The solution shall maintain linkage between the identified exposure, affected asset, remediation action and validation result throughout the exposure-management lifecycle.
9. The solution shall support tracking of remediation status, including open, remediated, and accepted-risk states.

10. The solution shall provide attack-path visualization showing relationships between affected assets, security weaknesses and potential paths to critical assets based on available integrated data.
11. The solution shall provide dashboards and reports covering key enterprise exposure metrics, including critical exposures, internet-facing assets, attack paths, and remediation trends, with support for customizable reporting.
12. The solution shall support filtering and drill-down of exposure information by business unit, asset, application, technology, environment, criticality, risk, exposure type and remediation status.
13. The solution shall support machine-readable and human-readable export of exposure information, risk assessments, validation results and remediation status.
14. The solution shall provide trend analysis to measure changes in overall exposure, critical exposures, validated exposures and remediation effectiveness over time.

7.3.14.2 Key Deliverables:

1. Solution Architecture Document
2. Enterprise Asset Inventory & Attack Surface Discovery Report.
3. Exposure Assessment & Risk Prioritization Report
4. Remediation Planning & Exposure Reduction Report
5. Executive Dashboards, Operational Dashboards, and Regulatory Compliance Reports.
6. Periodic Exposure Review & Risk Trend Report.

7.4 Functional Requirement - Services (Offsite Services)

a. In alignment with the regulatory guidelines and advisories, internal information security governance requirements, the Bank proposes to subscribe (Solution licenses are not to be procured) required to a set of specialized, off-site cyber services to enhance its external threat visibility and proactive defence capabilities.

b. These services are intended to complement the Bank's security controls by providing continuous intelligence, detection, and monitoring of threats originating outside the Bank's perimeter and digital infrastructure.

c. The Bidder shall ensure compliance with all applicable Government of India guidelines, RBI directives, CERT-In advisories, regulatory requirements, and the Bank's policies relating to data localization, data privacy, data sharing, and information security.

d. The Bidder shall implement appropriate security controls, including data masking or tokenization for sensitive data, Role-Based Access Control (RBAC), Just-in-Time (JIT) privileged access, and comprehensive audit logging for all services delivered under this RFP.

e. The proposed services should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.

f. The frequency and scope of each service shall be as specified in Annexure 21 – Sizing/Volumetrics.

g. All tools/platforms proposed for delivery of these services shall comply with the Bank's applicable information security, data protection, access control, logging, audit, and regulatory requirements.

h. All the proposed services should comply with Appendix 1C: Functional Compliance Sheet (Services)

7.4.1 Breach Attack & Simulation

The Bidder shall provide continuous Breach Attack & Simulation (BAS) services to validate the effectiveness of the Bank's preventive, detective, and response security controls by emulating real-world cyber-attack techniques across the Bank's IT environment.

The service shall include, wherever applicable:

- Continuous validation of security controls against known attack techniques.
- Assessment of security control effectiveness across network, endpoint, identity, application, cloud, and hybrid environments.
- Mapping of attack scenarios to MITRE ATT&CK
- Validation of detection, prevention, and response capabilities.
- Identification of control gaps, security weaknesses, and attack paths.
- Risk-based prioritization and remediation recommendations.
- Executive, operational, and technical reporting
- AI assisted attack path analysis, control gap identification and risk-based prioritization.

7.4.2 Continuous Automated Red Teaming Services

The Bidder shall conduct continuous automated Red Team exercises to simulate advanced threat actors and evaluate the effectiveness of the Bank's security controls, monitoring capabilities, incident response processes, cyber resilience, and operational readiness.
The service shall include:

- Testing of people, processes, and technology.
- Validation of SOC detection and incident response capabilities.
- Assessment of identity, network, cloud, application, endpoint, and AI attack vectors, wherever applicable.
- Attack path analysis and privilege escalation validation.
- Recommendations for improving cyber resilience.
- AI assisted automated attack simulation and attack path analysis
- The proposed solution shall provide Continuous Automated Red Teaming (CART) capabilities to continuously simulate real-world cyberattacks against the organization's attack surface, identify exploitable vulnerabilities and attack paths, validate the effectiveness of existing security controls, and provide risk-based, actionable remediation recommendations.

.

7.4.3 Attack surface management

The Bidder shall provide continuous discovery, monitoring, classification, and risk assessment of the Bank's internet-facing & external surface.
The service shall include:

- Discovery of internet-facing & external assets.
- Identification of exposed services, applications, domains, cloud assets, certificates, and digital infrastructure.
- Continuous exposure monitoring.
- Identification of misconfigurations and security exposures.
- Risk prioritization based on business impact.
- Recommendations for attack surface reduction.
- The proposed solution shall provide AI-enabled Attack Surface Management (ASM) capabilities for continuous discovery, identification, monitoring, assessment, and risk-based prioritization of the organization's external attack surface, including known and unknown internet-facing assets. The solution shall identify vulnerabilities, misconfigurations, security exposures, and associated risks, and provide actionable remediation recommendations.

.

7.4.4 Phishing Simulation

The Bidder shall provide offsite, tool-based phishing simulation services to assess employee awareness, measure the Bank's resilience against phishing attacks, and support continuous improvement of security awareness.

The service shall be delivered through a centralized platform/tool and shall include, but not be limited to:

Conducting controlled and customizable simulated phishing campaigns.

- **a.** User awareness and susceptibility assessment.
- **b.** Behavioural analysis of users' responses to simulated phishing campaigns.
- **c.** Department-wise and user-wise risk assessment.
- **d.** Campaign-wise and periodic awareness effectiveness reporting.
- **e.** Identification of high-risk users and trends.
- **f.** Recommendations for improving employee security awareness including training.
- **g.** Dashboard-based visibility of campaign status, results, user responses, and risk metrics.
- **h.** Generation of management and executive reports as required by the Bank.
- **i.** AI based user behaviour and phishing susceptibility analysis
- **j.** AI based detection and classification of phishing and impersonation threats.
- **k.** AI based analysis and correlation of exposed credentials, data leaks and threat indicators.
- **l.** AI based enrichment, correlation and prioritization of threat intelligence
- **m.** AI based behavioural analytics, anomaly detection and threat correlation

7.4.5 Anti-Phishing

This clause stands deleted. The Anti-Phishing services have been moved under the Digital Risk Management scope.

7.4.6 Dark Web Monitoring

The Bidder shall provide offsite, tool-based continuous dark web and cyber threat exposure monitoring services to identify potential exposure of the Bank's sensitive information across the surface web, deep web, dark web, underground forums, messaging platforms, and data leak repositories.

The service shall include, but not be limited to:

- **a.** Continuous monitoring for credential exposure.
- **b.** Monitoring for sensitive information and data leakage.
- **c.** Monitoring of employee and executive exposure.
- **d.** Monitoring for financial fraud indicators and relevant threat activities.
- **e.** Monitoring of compromised accounts, credentials, and other exposed information.
- **f.** Threat intelligence correlation and contextual analysis.
- **g.** Risk assessment and prioritization of identified exposures.
- **h.** Timely notification of critical or high-risk exposures.
- **i.** Dashboard-based visibility of identified exposures and their status.
- **j.** Periodic and ad-hoc risk and exposure reports.

7.4.7 Threat Intelligence Feed

The Bidder shall provide offsite, tool-based, curated, contextual, and actionable cyber threat intelligence services relevant to the Bank's threat landscape.

The service shall include, but not be limited to:

- **a.** Indicators of Compromise (IOC).
- **b.** Indicators of Attack (IOA).
- **c.** Threat actor and campaign intelligence.
- **d.** Malware and ransomware intelligence.
- **e.** Vulnerability and exploit intelligence.

f. AI-related threat intelligence, wherever applicable.
g. Threat intelligence related to the banking and financial services sector.
h. MITRE ATT&CK mapping of relevant threats and adversary techniques.
i. Threat intelligence enrichment, correlation, and contextualization.
j. Threat prioritization based on relevance and risk to the Bank.
k. Actionable recommendations for detection, prevention, and mitigation.
l. Provision of threat intelligence through a centralized portal/dashboard and/or machine-readable feeds
m. Periodic threat intelligence reports and alerts.

7.4.8 Threat Hunting Services

The Bidder shall provide offsite, tool-based, proactive and intelligence-driven threat hunting services to identify advanced threats, malicious activities, unknown attack techniques, and indicators of compromise that may evade the Bank's existing security controls.
The service shall include, but not be limited to:

a. Proactive threat hunting across endpoint, network, cloud, identity, application, and AI environments, wherever applicable.
b. IOC, IOA, and TTP-based investigation.
c. Behavioural analytics and anomaly detection.
d. Threat intelligence-driven threat hunting.
e. Investigation of suspected advanced persistent threats and emerging attack techniques.
f. Detection engineering and security use-case tuning.
g. Correlation rule optimization.
h. Validation and assessment of SOC detection capabilities.
i. Identification of gaps in existing detection and monitoring mechanisms.
j. Recommendations for remediation and improvement of security controls.
k. Periodic threat hunting reports, findings, risk assessment, and executive dashboards.
l. Tracking of identified findings and recommended remediation actions.
m. The threat hunting service shall be delivered remotely/offsite using secure and mutually agreed mechanisms for accessing relevant logs, telemetry, security tools, and data made available by the Bank.

7.4.9 Brand Protection and Monitoring (Brand Abuse)

This clause stands deleted. The Brand Abuse services have been moved under the Digital Risk Management scope.

7.4.10 Digital Risk management

The bidder shall provide offsite Digital risk management services for identifying and taking down phishing websites / rogue applications, brand abuse etc.
Digital Risk Management – Comprising of Anti Phishing and brand Abuse and management

The Bidder shall provide offsite, tool-based Digital Risk Management (DRM) services for continuous identification, monitoring, analysis, validation, risk assessment and remediation of digital risks associated with the Bank, including its digital assets, domains, websites, mobile applications, social media presence, brand and other online channels.

The service shall include, but not be limited to:

a. Continuous monitoring of the Bank's external digital presence, including domains, websites, mobile applications, social media presence and other identified digital assets
b. Brand Protection: Identification and monitoring of unauthorized use, misuse or impersonation of the Bank's brand elements across relevant online channels.

c. Anti-Phishing: Continuous detection and monitoring of phishing websites, malicious URLs, fraudulent websites and other phishing-related digital threats targeting the Bank or its customers.
d. Rogue Application Monitoring: Monitoring and identification of fraudulent, counterfeit, malicious or impersonating mobile applications across relevant application marketplaces, including support for appropriate removal or takedown actions.
e. Detection and Intelligence: Utilization of relevant intelligence, analytics and other applicable technologies for identified digital risk.
f. Takedown and Remediation: Support for takedown and remediation of identified phishing websites, fraudulent or malicious domains, rogue applications, impersonation.
g. Reporting and Dashboards: Provision of dashboards and periodic or on-demand reports covering Anti-phishing and brand abuse services

7.5 Bidder Responsibilities

1. The Bidder shall prepare and submit a detailed implementation plan covering project governance, implementation methodology, timelines, milestones, resource deployment, risk management, rollback strategy, and cutover plan.
2. The Bidder shall assess the Bank's existing environment and ensure seamless deployment, migration, and interoperability with the Bank's current infrastructure as well as its target IT and Cyber Security architecture.
3. The Bidder shall factor all activities required for successful implementation, including sizing, capacity planning, Bill of Materials (BoM) validation, supply, installation, rack mounting, cabling, commissioning, configuration, testing, migration, integration, and go-live, without any additional cost to the Bank.
4. The Bidder shall ensure seamless integration of the proposed solution with existing and future Bank systems through standard APIs, connectors, log forwarding mechanisms, and other interoperability interfaces, including integration with SIEM, SOAR, Identity Services, Threat Intelligence Platforms, ITSM, and other security solutions, wherever applicable.
5. The Bidder shall perform operating system hardening, secure configuration, backup configuration, disaster recovery readiness, monitoring, alerting, dashboards, reporting, and automated notification configuration in accordance with the Bank's security policies and industry best practices.
6. The Bidder shall provide complete implementation documentation, configuration records, audit trails, operational procedures, and knowledge transfer to the Bank's administrators and operations teams.
7. The Bidder shall coordinate with OEMs, cloud service providers, third-party vendors, telecom service providers, and Bank stakeholders throughout implementation, migration, testing, and issue resolution.
8. The Bidder shall provide post go-live stabilization support, periodic health checks/Architecture assessment, configuration review, performance tuning, patch management, firmware/software upgrades, signature updates, and technical support throughout the warranty, ATS, AMC, and Operations & Maintenance (O&M) period.
9. The Bidder shall establish a 24×7 technical support and escalation mechanism for incident management and timely resolution throughout the contract period.

7.6 OEM Responsibilities

1. All activities relating to solution architecture, design, implementation, configuration, customization, integration, migration, testing, deployment, documentation, training, and Go-Live shall be performed by the respective Solution OEM in coordination with the Bidder.
2. The OEM shall design, implement, and support an enterprise-grade, scalable, resilient, secure, and future-ready solution compatible with the Bank's existing and target IT and Cyber Security architecture across on-premises, cloud, and hybrid environments.
3. The OEM shall prepare and submit all design documents including HLD, LLD, deployment architecture, integration architecture, configuration guides, SOPs, operational manuals, as-built documentation, and implementation artefacts.
4. The OEM shall provide all native and custom integrations, APIs, connectors, parsers, workflows, playbooks, dashboards, reports, automation, authentication, authorization, RBAC, logging, monitoring, alerting, and interoperability required for successful operation of the solution.
5. The OEM shall perform sizing validation, deployment, migration, configuration, tuning, optimization, health checks, and stabilization to ensure successful commissioning of the solution.
6. The OEM shall support SIT, UAT, performance validation, security validation, regulatory audits, compliance assessments, and remediation of observations relating to the proposed solution.
7. During Warranty, ATS, AMC, and O&M, the OEM shall provide highest-level technical support, periodic architecture reviews, configuration reviews, policy optimization, health assessment, and technology roadmap recommendations.
8. The OEM shall implement all Bank-approved policy changes, configurations, enhancements, integrations, parsers, playbooks, workflows, reports, dashboards, automation, tuning, and customization throughout the contract period without additional cost.
9. The OEM shall maintain and periodically (Quarterly or as required by regulators) update Software Bill of Materials (SBOM), Cryptographic Bill of Materials (CBOM), Quantum Bill of Materials (QBOM), AI Bill of Materials (AI-BOM), and all dependent components in accordance with applicable CERT-In guidelines and regulatory requirements.
10. The OEM shall submit Go-Live, Acceptance, Handover, and Operational Readiness Reports prior to project closure..

7.6.1 Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder)

1. The respective Solution OEM, assisted by the bidder, shall conduct a detailed assessment of the Bank's business, functional, technical, operational, security, compliance, and integration requirements and design a scalable, resilient, and future-ready solution. The proposed solution shall fully comply with the requirements specified in the RFP and support future business and technology needs of the Bank.
2. As part of the requirement gathering phase, the OEM shall conduct workshops, discovery sessions, interviews, and discussions with the Bank's stakeholders and appointed consultants to understand business requirements, existing infrastructure & solutions, integrations, operational processes, and security requirements.
3. The OEM shall review the Bank's existing IT, security, application, network, cloud, and infrastructure landscape and recommend an optimized target-state architecture leveraging both existing and proposed components wherever feasible.

4. The OEM shall identify all required data sources, integrations, dependencies, interfaces, telemetry sources, and compliance requirements and prepare a detailed solution architecture and deployment design in consultation with the Bank.
5. The scope shall include, but not be limited to:
    a. Requirements elicitation and analysis
    b. Gap assessment and solution mapping
    c. Leveraging standard product capabilities, policies, rules, parsers, controls, and automation features
    d. Identification of functional, technical, operational, security, reporting, and integration requirements
    e. Definition of data sources, use cases, workflows, dashboards, reports, and analytics requirements
6. The bidder and OEM shall coordinate with the Bank's internal teams, existing vendors, OEMs, and service providers to gather information required for integration, migration, deployment, and operationalization of the proposed solution. The Bank shall facilitate necessary coordination wherever required.
7. The bidder and OEM shall prepare and submit a Functional Requirement Specification Manual (FRSM) covering all agreed functional, technical, integration, reporting, operational, security, and compliance requirements. The FRSM shall be reviewed by the Bank, and any observations or approved additions shall be incorporated prior to finalization.
8. The bidder and OEM shall implement and deliver all functionalities, integrations, software, hardware, licenses, infrastructure components, and services required to meet the requirements defined in the approved FRSM, RFP, and associated project documents.

7.6.2 System Design - Activities are to be performed by Respective solution OEM (supported by bidder)

1. The bidder and respective OEM shall be responsible for the end-to-end design, sizing, customization, configuration, integration, implementation, deployment, maintenance, and support of the proposed solution, including coordination with all associated OEMs, service providers, and stakeholders.
2. All proposed NextGEN SOC solutions shall support seamless interoperability, real-time integration, event sharing, correlation, orchestration, and automated response capabilities to enable unified security operations and minimize manual intervention.
3. The proposed solution shall be configurable and customizable to meet the Bank's functional, technical, operational, reporting, security, and compliance requirements.
4. The bidder and OEM shall design and implement a secure, scalable, resilient, and future-ready architecture based on the approved requirements, data flows, integrations, and operational needs of the Bank.
5. The bidder and OEM shall prepare and submit the following design documents for Bank approval:
    a. High-Level Design (HLD), including solution architecture, deployment architecture, integration architecture, and data flow architecture.
    b. Low-Level Design (LLD), including detailed technical specifications, interface specifications, deployment details, configuration standards, and integration mechanisms.
    c. Technical architecture documentation covering processes, interfaces, deployments, data flows, transformations, reporting, security controls, and operational workflows.
6. The bidder and OEM shall be responsible for implementation of all solution components, integrations, interfaces, workflows, automation, business rules,

exception handling, logging, monitoring, archival mechanisms, data exchanges, deployment activities, and testing required for successful commissioning of the solution.

7. The bidder and OEM shall ensure seamless integration with the Bank's internal systems, external entities, regulatory interfaces, fintech partners, and third-party applications through standards-based and scalable integration mechanisms, enabling future expansion through a plug-and-play model.
8. The bidder shall remain fully accountable for successful end-to-end solution delivery and achievement of all functional, technical, operational, performance, security, and compliance requirements specified in the RFP.

7.6.3 Development and Installation - Activities are to be performed by Respective Solution OEM (supported by bidder)

1. All installation, configuration, customization, testing, migration, integration, UAT, Go-Live, and related implementation activities shall be performed from the Bank's premises.
2. The bidder and respective OEM shall integrate the proposed solution with the Bank's ITSM, SLA Monitoring, monitoring, logging, authentication, and other enterprise platforms, as required.
3. The bidder and OEM shall coordinate with all relevant third parties, OEMs, service providers, and Bank stakeholders to ensure seamless integration, interoperability, and end-to-end functionality of the proposed solution.
4. The bidder shall provide all required integrations, connectors, parsers, APIs, workflows, playbooks, dashboards, reports, alerts, fine-tuning, customizations, enhancements, and remediation activities necessary for successful operation of the solution throughout the contract period without any additional cost to the Bank.
5. The bidder shall adopt and submit an implementation methodology covering solution deployment, customization, testing, managed services, facility management services, knowledge transfer, and hardware/software installation and configuration activities.
6. The proposed solution shall be complete in all respects and shall not require any additional third-party software, licenses, tools, or components beyond those proposed under this RFP. Any such dependencies shall be identified, supplied, implemented, and commercially included by the bidder.
7. The solution and associated services shall comply with applicable regulatory, statutory, and industry standards, including RBI guidelines, DPDP requirements, Government of India directives, PCI-DSS, ISO standards, and other applicable compliance requirements.
8. The implementation approach shall clearly define inputs, activities, outputs, deliverables, tools, templates, timelines, review mechanisms, and sign-off procedures for each phase of the project.
9. The bidder shall adhere to established quality management, project governance, and risk management practices and shall provide the necessary templates, processes, and controls for effective project execution.
10. The implementation scope shall include requirement gathering, SRS/FRS preparation, customization, installation, configuration, integration, testing, migration, cutover, Go-Live, stabilization, and knowledge transfer activities.
11. The bidder shall ensure active participation of its personnel and OEM resources throughout the implementation lifecycle to facilitate effective knowledge transfer and operational readiness of the Bank's teams.
12. The bidder shall size, provision, implement, and support the required IT infrastructure in accordance with the RFP requirements. Any shortfall in sizing, capacity,

performance, availability, or scalability identified during implementation or the contract period shall be rectified by the bidder at no additional cost to the Bank.

13. The proposed solution shall support integration and interoperability with the Bank's existing security ecosystem as well as security solutions being implemented under this or other Bank initiatives, ensuring a unified and future-ready cybersecurity architecture.

7.6.4 Documentation - Activities are to be performed by Respective solution OEM (supported by bidder)

The bidder and respective OEM shall prepare, maintain, obtain Bank approval/sign-off, and submit all project, technical, operational, security, and administrative documentation associated with the proposed solution. The indicative list of deliverables shall include, but not be limited to, the following:

1. Detailed Project Plan and Implementation Plan
2. Hardware, Software, Infrastructure, and Sizing Specifications
3. High-Level Design (HLD) and Low-Level Design (LLD) Documents
4. Solution Architecture, Deployment Architecture, and Data Flow Documents
5. Secure Configuration Standards, Baseline Hardening Documents, and Security Configuration Guides
6. System, Database, Integration, Troubleshooting, Diagnostics, and Maintenance Documents
7. Testing, Validation, Acceptance, and Go-Live Documents
8. Change Management, Release Management, Problem Management, and Operational Procedures
9. User Management, Access Management, and Role Administration Guides
10. Release Notes, Impact Assessment Matrix, and Dependency Mapping Documents
11. Backup, Recovery, Business Continuity, and Disaster Recovery Procedures
12. User, Installation, Operations, Technical, and Administration Manuals
13. Knowledge Transfer Documents, SOPs, Run Books, and Knowledge Articles
14. The Secure Configuration Documents (SCDs) and Baseline Hardening Standards for all in-scope solutions shall be reviewed at least quarterly, updated as required, maintained under version control, and submitted to the Bank for review and approval.

7.6.5 Deployment and Go-Live - Activities are to be performed by Respective Solution OEM (supported by bidder)

1. The bidder and respective OEM shall be responsible for deployment of the solution in the production environment, Go-Live planning, implementation, installation, configuration, fine-tuning, migration, stabilization, and hyper care support.
2. The Bidder and respective OEM shall deploy & implement bank's identified existing security rules, policies, use cases, configuration, and other learnings from bank's existing technologies/solutions.
3. The bidder and OEM shall provide onsite support during the hyper care period, monitor solution performance, assist users, conduct training sessions, address issues and defects, implement corrective actions, and recommend operational best practices.
4. The implementation scope shall include deployment planning, migration, testing, validation, issue resolution, user acceptance support, Go-Live execution, and post-Go-Live stabilization activities.
5. Prior to Go-Live, the solution shall undergo security validation activities, including VAPT, IS Audit, readiness assessments, identification of security gaps and blind spots, risk remediation, and implementation of recommendations. The Bank or its

appointed agency may conduct Continuous Automated Red Teaming, Purple Teaming, security assessments, or other validation exercises as deemed necessary.

6. The bidder and OEM shall conduct performance testing prior to UAT and Go-Live to validate that the proposed solution can meet the Bank's performance, scalability, availability, and capacity requirements under normal, peak, and stress conditions.
7. Performance testing shall include, at a minimum:
    - Load Testing
    - Stress Testing
    - Scalability Testing
    - Endurance Testing
    - Failover and Recovery Testing
8. The bidder shall measure and report key performance indicators including, but not limited to:
    - Response Time
    - Throughput
    - CPU, Memory, Disk, and Network Utilization
    - Error Rates
    - System Recovery and Restoration Time
    - Solution Availability and Stability Metrics
9. The performance testing lifecycle shall include planning, test design, environment preparation, execution, monitoring, analysis, tuning, optimization, and re-testing activities. Any performance bottlenecks, defects, or capacity constraints identified during testing shall be rectified by the bidder at no additional cost to the Bank.

7.6.6 Testing- Activities are to be performed by Respective solution OEM (supported by bidder)

1. The Bank shall conduct User Acceptance Testing (UAT) to validate that the proposed solution and all associated components, integrations, workflows, reports, dashboards, and functionalities comply with the requirements specified in the RFP, approved FRSM/SRS, and other project documents.
2. The bidder and respective OEM shall confirm completion of all implementations, configuration, customization, integration, migration, and testing activities prior to commencement of UAT and certify that the solution is ready for user validation.
3. Any defects, deviations, vulnerabilities, observations, or non-compliances identified during UAT, security assessments, audits, reviews, or validation exercises shall be rectified by the bidder within the timelines prescribed by the Bank and at no additional cost.
4. The bidder shall maintain appropriate version control, configuration management, change management, release management, and documentation controls throughout the implementation and testing lifecycle.
5. The bidder shall update all technical, operational, security, user, and administrative documentation to reflect changes, enhancements, configurations, fixes, and upgrades implemented during the project.
6. The bidder shall remediate security vulnerabilities, gaps, weaknesses, audit observations, and control deficiencies identified during implementation, testing, assessments, audits, reviews, or operational activities, subject to Bank approval wherever required.
7. During the contract period, the bidder shall support periodic reviews, assessments, audits, and compliance validation activities, as required by the Bank, including but not limited to:
    - Policies, procedures, and governance controls
    - IT General Controls (ITGC)

- Logical Access Management and Privileged Access Management
- Physical and Environmental Security Controls
- Change and Release Management Processes
- Third-Party and Vendor Management Controls
- Backup, Recovery, and Data Protection Controls
- Incident Management Processes
- Business Continuity and Disaster Recovery Arrangements
- Security Configurations and Hardening Standards
- Operating Systems, Databases, Applications, Network Devices, Security Devices, and Cloud Infrastructure Security Reviews

8. The bidder shall provide all necessary support, documentation, evidence, reports, logs, and resources required for successful completion of such reviews, assessments, audits, and compliance activities.

7.6.6.1 Quality Assurance

1. Testing Requirements
   a. The respective OEM shall be responsible for planning, executing, documenting, and successfully completing all testing activities required to validate the functionality, performance, stability, reliability, security, interoperability, and operational readiness of the proposed solution. The bidder shall prepare detailed test plans, test cases, test data, automation scripts (where applicable), entry and exit criteria, test reports, defect logs, root cause analysis reports, workarounds, and remediation plans, and shall obtain the Bank's approval wherever required.
2. Test Preparation
   The respective OEM shall:
   a. Prepare the overall testing strategy and methodology for Unit Testing (UT), UAT, Performance Testing, Security Testing, and other applicable tests.
   b. Establish and maintain the required test environments, infrastructure, software, applications, and test data.
   c. Prepare, validate, and execute test cases, scripts, and automation frameworks, wherever applicable.
   d. Define test entry and exit criteria, acceptance criteria, and success parameters.
3. Test Execution
   The respective OEM shall:
   a. Execute all approved test cases and scripts.
   b. Record, track, report, and resolve defects, deviations, and observations.
   c. Perform re-testing and regression testing after issue resolution.
   d. Submit test results, defect reports, execution evidence, and test summary reports in formats approved by the Bank.
   e. Provide recommendations for usability, performance improvements, operational enhancements, and risk mitigation.
4. Types of Testing
   The respective OEM shall perform, at a minimum, the following testing activities, wherever applicable:
   a. Unit Testing (UT)
   b. User Acceptance Testing (UAT) Support
   c. Functional Testing
   d. Performance, Load, Stress, Volume, and Scalability Testing
   e. Security and Configuration Validation Testing

f. Data Migration Testing
g. Interface and Integration Testing
h. Compatibility and Interoperability Testing
i. Exception Handling and Failover Testing
j. Installation and Upgrade Testing
k. Regression and Sanity Testing
l. Operational Readiness Testing
m. Usability Testing
n. Any other testing required to ensure successful implementation and acceptance of the solution
o. The bidder & OEM shall rectify all defects, vulnerabilities, configuration issues, integration issues, performance bottlenecks, and non-compliances identified during testing at no additional cost to the Bank. Successful completion of all testing activities and closure of observations shall be a prerequisite for progression to subsequent project phases and Go-Live approval.

7.6.7 Training- Activities are to be performed by Respective solution OEM (supported by bidder)

HANDHOLDING

The Bidder/OEM shall provide **post-Go-Live handholding, operational support and configuration-level knowledge transfer/training** to the Bank's designated bank's team for each proposed solution/services.

TRAINING

Training may be delivered through **Computer-Based Training (CBT), Online Instructor-Led Training (ILT), or OEM Online Training**

The Bidder and Respective OEM shall provide product-specific training and certification for the Bank's nominated personnel throughout the contract period.

- **Year 1 / Post Go-Live:** Minimum **40 hours of training per proposed Solution/Service** shall be provided. **CBT/OEM Online Training shall be the preferred mode**; where CBT/OEM Online Training is not available, **Instructor-Led Training (ILT)** shall be provided for a minimum of 40 hours.
- **CBT/OEM Online Training:** The Year-1, post Go-live, training content shall comprise a minimum of **40 hours of material** and shall remain accessible to the Bank for at least **six (6) months for completion of certification & learning**.
- **Annual Refresher Training:** A minimum of **16 hours of training per proposed Solution/Service per year** shall be provided during subsequent years. CBT/OEM Online Training shall be provided, where available, and shall remain accessible for at least **one (1) month**. Where CBT is unavailable, **ILT of minimum 16 hours** shall be provided for each proposed **Solution/Service**.
- Training shall cover relevant product functionality, administration, configuration, operation, troubleshooting, new features and significant product updates, as applicable.
- Certification shall be issued by the respective OEM upon successful completion of the prescribed training and assessment
- The minimum training entitlement shall apply **to each proposed Solution/Service**.

CERTIFICATION:

Training & Certification arranged by the Bidder only in 1st Year

Only 1 Certification training should be provided in Beginner and Advance for respective Domain.

Domain	Beginner / Foundation (Only 1 Certification in Each Domain)	Advanced / Specialist (Only 1 Certification in Each Domain)
Cloud Security	• Microsoft Azure, Google Cloud, AWS Cloud Security Certificate.	• AWS Certified Security – Specialty; • Microsoft Certified: Cybersecurity Architect Expert (SC-100) • Google Professional Cloud Network Engineer
Threat Hunting	Certified Network Defender (CND) Or any other relevant certification	Certified Cyber Threat Hunting Professional (CCTHP) Or any other relevant certification
Detection Engineering	• Certified Security Operations Analyst (CSA); • Microsoft Security Operations Analyst (SC-200); • Splunk Core Certified Power User; Elastic Certified Analyst • Or any other relevant certification	• Splunk Enterprise Certified Administrator; • Splunk Enterprise Security Certified Administrator; • Elastic Certified Engineer; Google Chronicle Security Operations; • Palo Alto Networks Cortex XSIAM/XDR certifications • Microsoft Sentinel certifications/training • Or any other relevant certification
Cloud Incident Response and Forensics	• Microsoft Security Operations Analyst (SC-200); • Azure Security Engineer (AZ-500) • Or any other relevant certification	• AWS Certified Security – Specialty; • AWS Certified Advanced Networking – Specialty; • Google Professional Cloud Security Engineer • Or any other relevant certification
Threat Intelligence / Cyber Threat Intelligence	• Certified Threat Intelligence Analyst (CTIA); • Certified Threat Intelligence Professional (C|TIP) • Or any other relevant certification	• Certified Cyber Threat Hunting Professional (CCTHP) • Or any other relevant certification
Incident Response	• Microsoft Security Operations Analyst (SC-200) • Or any other relevant certification	• EC-Council Certified Incident Handler (ECIH) • Or any other relevant certification

The Bidder shall ensure access to the OEM's training/online platform, course material, assessments and certification examinations. The training shall cover relevant product administration, configuration, troubleshooting, security operations, monitoring, investigation, threat detection/hunting and other applicable functionalities.

The Bidder shall provide **OEM-recognized training and certification for 15 Bank officials for each respective solution**.

Failure to complete the stipulated training and certification within the prescribed timeline shall attract applicable LD as specified in the RFP.

The Bank reserves the right to nominate participants for the training programs and request additional refresher or knowledge transfer sessions during the contract period, wherever required.

7.6.8 Security requirements - Activities are to be performed by Respective Solution OEM (supported by bidder)

1. The bidder and respective OEMs shall comply with the Bank's IT, Information Security, Cyber Security, Data Protection, Privacy, Business Continuity, and related policies, standards, procedures, and guidelines, as shared by the Bank from time to time. The bidder shall be responsible for ensuring the confidentiality, integrity, availability, security, and privacy of the Bank's information assets, systems, applications, and data throughout the contract period.
2. The bidder shall implement and maintain appropriate administrative, technical, physical, and operational controls for protection of data, applications, systems, infrastructure, and associated assets under its custody or management.
3. The bidder shall comply with the Bank's requirements relating to access management, privileged access management, password policies, user administration, data protection, encryption, monitoring, incident management, and security governance.
4. The bidder shall ensure encryption and protection of data at rest, data in transit, and data in use, wherever applicable, using industry-standard security controls and cryptographic mechanisms. All tools, technologies, and controls required to achieve the same shall form part of the proposed solution.
5. The bidder and OEM shall comply with all applicable regulatory, statutory, legal, and industry requirements, including RBI & GOI guidelines, DPDP Act, CERT-In advisories, and other applicable cybersecurity and data protection requirements.
6. All Bank data, including production data, backup data, logs, telemetry, monitoring information, license-related data, and any other information generated, processed, transmitted, or stored by the proposed solution, shall reside within India. No Bank data shall be transmitted, replicated, processed, accessed, stored, or exchanged outside India without prior written approval from the Bank and applicable regulatory permissions.
7. The bidder shall ensure that Personally Identifiable Information (PII), sensitive personal data, financial information, and other confidential information are appropriately masked, encrypted, protected, and accessible strictly on a need-to-know basis in accordance with the Bank's access control policies.
8. The bidder shall provide all logs, records, evidence, reports, forensic artifacts, and other information required by the Bank for security investigations, regulatory reviews, audits, incident response activities, and forensic analysis.
9. The bidder shall promptly report information security incidents, cyber incidents, breaches, vulnerabilities, and control failures affecting the proposed solution and shall provide detailed incident reports, root cause analysis, corrective actions, and preventive measures.

10. The bidder and OEM shall establish, implement, and maintain secure baseline configurations and hardening standards for all operating systems, databases, applications, network devices, security devices, middleware, cloud resources, and supporting infrastructure and shall periodically review and update the same in accordance with industry best practices.
11. The Bank or its authorized representatives shall have the right to conduct audits, reviews, assessments, inspections, and compliance validation activities relating to the proposed solution, associated processes, controls, facilities, personnel, documentation, and supporting infrastructure. The bidder shall provide all necessary cooperation, access, information, records, and assistance required for such activities.

7.7 On-cloud proposed solution OEM Responsibilities

The requirements contained in this section apply to all cloud-hosted solutions.
However, the bidder and OEM shall remain fully accountable to the Bank for compliance with all contractual, security, operational, regulatory, and performance requirements specified in this RFP.

1. The security telemetry received by the OEM Cloud platform will be routed to the dedicated logical tenant/workspace provisioned for the Bank.
2. The dedicated tenant/workspace will contain the configurations, policies, security data and analytics applicable to the Bank.
3. All security logs, telemetry, alerts, incidents, configurations, investigation data and other Bank-related security information stored in the Cloud environment shall be encrypted at rest using industry-standard encryption mechanisms.
4. The proposed Cloud/SaaS solution shall support Bring Your Own Key (BYOK) and/or Customer-Managed Encryption Key (CMEK) capability, enabling the Bank to maintain control over the cryptographic keys used to protect its security data.
5. The encryption key will be securely managed and access to the key will be restricted to authorised personnel/processes.
6. The bidder/OEM shall establish and manage a dedicated cloud landing zone, including Development, UAT, and Production environments, with appropriate segregation, governance, access controls, monitoring, and SDLC controls.
7. The bidder/OEM shall be responsible for provisioning, configuration, administration, monitoring, patching, upgrading, backup, recovery, migration, and lifecycle management of all cloud resources, including compute, storage, databases, containers, networking, security services, and associated cloud components.
8. The solution shall support secure connectivity with the Bank's on-premises infrastructure, cloud environments, and external systems through private or secure communication mechanisms via internet, or the tenant can be restricted based on Bank's static public IP addresses.
9. The bidder shall ensure compliance with applicable RBI guidelines, DPDP requirements, NCIIPC, CERT-In advisories, Government of India regulations, Bank policies, and other applicable regulatory, statutory, and industry standards. Necessary compliance artefacts, audit evidence, risk assessments, reports, and documentation shall be maintained and provided to the Bank as required by bidder/OEM on regular basis as well as whenever required.
10. The OEM shall have valid ISO/IEC 27001 certification and SOC 2 Type II report.
11. All Bank data, including production data, backups, logs, telemetry, prompts, metadata, and related information, shall reside within India. No data shall be transmitted, processed, stored, validated, replicated, or accessed outside India without prior written approval from the Bank and applicable regulatory authorities.
12. The bidder and OEM shall provide complete data ownership, data sovereignty, confidentiality, and privacy of the Bank's information. Bank data shall not be used for

model training, model retraining, analytics, or shared with third parties, whatsoever, except as explicitly authorized by the Bank in writing.

13. The solution should provide encryption of data at rest, motion, and in transit using industry-standard cryptographic controls and shall support key management through CSP-native KMS and/or the Bank's Key Management System.
14. The provisioned environment shall provide comprehensive monitoring, logging, audit trails, governance controls, compliance reporting, security event monitoring, and forensic investigation capabilities through centralized dashboards and reporting mechanisms to the bank.
15. The cloud platform shall support high availability, fault tolerance, disaster recovery, multi-site deployment, backup and recovery services, and business continuity capabilities in accordance with the Bank's RTO, RPO, availability, and resilience requirements.
16. The bidder shall provide enterprise-grade support services, including 24x7 support, incident management, escalation management, defined service levels, and proactive operational support throughout the contract period.
17. The bidder shall be responsible for sizing all cloud resources, including compute, containers, databases, storage, caching, networking, API gateways, load balancers, egress/ingress and related services. Any capacity shortfall affecting performance, scalability, availability, or SLA compliance shall be addressed by the bidder at no additional cost to the Bank.
18. The bidder shall provide periodic utilization, performance, capacity, availability, security, backup, and SLA compliance reports for all cloud-hosted services as per the reporting requirements defined in the RFP.
19. The cloud platform shall provide native audit logging, security monitoring, vulnerability management, backup management, access management, and security controls necessary for secure operation of the proposed solution throughout the contract period.
20. If, at any time during the contract period or during any audit, assessment, review, inspection, or compliance validation exercise, any deviation, non-compliance, deficiency, or control gap is identified, the bidder shall promptly rectify the same within the timeline prescribed by the Bank. Until such deviation or non-compliance is fully remediated and accepted by the Bank, the bidder shall remain liable for applicable penalties, and other contractual remedies as specified in the RFP and contract.
21. The bidder shall submit compliance against the Technical Specifications – Sheet Name: Cloud Deployment Requirement for every solution proposed under cloud deployment models. The compliance shall clearly demonstrate that the proposed cloud environment, associated services, and all supporting components, including the proposed solution, fully meet the technical, security, operational, regulatory, and contractual requirements specified in this RFP.

7.8 Non-functional requirements

The bidder shall ensure that the proposed solution architecture is secure, scalable, resilient, interoperable, future-ready, and aligned with industry best practices, regulatory requirements, and the Bank's business and technology objectives. The following architectural principles shall, at a minimum, be considered:

1. Industry Best Practices: The solution shall be implemented in accordance with industry-recognized standards, frameworks, and best practices and shall be appropriately configured and customized to meet the Bank's requirements.
2. Proven Technologies: The proposed solution shall comprise mature, proven, and enterprise-grade products and technologies with demonstrated deployments in comparable environments.

3. Scalability: The solution shall support seamless horizontal and/or vertical scalability to accommodate growth in users, transactions, workloads, data volumes, integrations, and business requirements without service degradation.
4. Interoperability: The solution shall support open standards, APIs, and industry-standard integration mechanisms to enable interoperability, portability, and seamless integration with existing and future systems.
5. Availability and Resilience: The solution shall incorporate appropriate redundancy, fault tolerance, high availability, and disaster recovery capabilities to support continuous operations and minimize service disruption.
6. Reliability: The solution shall ensure data integrity, operational stability, business continuity, and consistent performance throughout the contract period.
7. Security by Design: The solution shall support robust security controls, including role-based access control, authentication, authorization, encryption of data at rest, in transit, and in use, logging, monitoring, auditability, and other security measures as required by the Bank.
8. Technology Currency and Supportability: All proposed software, hardware, subscriptions, and services shall be based on the latest stable and OEM-supported versions available at the time of implementation and shall remain supported by the OEM throughout the contract period.
9. Compliance: The bidder and OEM shall comply with the Bank's IT, Information Security, Cyber Security, Data Governance, Data Retention, Privacy, and related policies, standards, procedures, and regulatory requirements at all times.

7.9 Delivery, Installation & Commissioning

1. The bidder shall ensure proper packaging, handling, transportation, storage, and delivery of all hardware, software, appliances, licenses, and associated components to prevent damage, deterioration, or loss. All products supplied shall be brand new, unused, genuine, and delivered in original OEM factory-sealed packaging.
2. The bidder shall complete delivery, installation, configuration, integration, testing, commissioning, and operationalization of the proposed solution at the designated Bank locations within the timelines specified in the RFP and the approved project plan.
3. Delivery shall be deemed complete upon receipt of all ordered hardware, software, licenses, firmware, documentation, and associated components at the designated Bank location(s) in good condition.
4. Installation, commissioning, and final acceptance shall be deemed complete only upon successful deployment, configuration, integration, testing, acceptance testing, demonstration of all functional, technical, interoperability, performance, and security requirements specified in the RFP, followed by formal sign-off by the Bank.
5. The bidder shall rectify all defects, deficiencies, non-compliances, performance, integration, or operational issues identified during implementation, testing, commissioning, acceptance, warranty, or operationalization by undertaking necessary repair, replacement, upgrade, augmentation, or corrective action at no additional cost to the Bank.
6. The bidder shall provide all contractual, commercial, licensing, warranty, insurance, technical, installation, operational, and support documentation, including documentary evidence of OEM authorization, licensing rights, warranty, support arrangements, and perpetual usage rights wherever applicable.

7. All software, firmware, licenses, subscriptions, and related components supplied under the contract shall be genuine, legally procured, appropriately licensed, and fully supported by the respective OEMs throughout the contract period.
8. Ownership of all supplied hardware, software licenses, subscriptions, entitlements, documentation, and other assets procured under this RFP shall vest with the Bank upon successful delivery and acceptance. For perpetual software licenses, the Bank shall receive the ownership/licensing and usage rights specified in the contract. For subscription-based or SaaS solutions, the Bank shall receive the contracted subscription, service and usage entitlements for the entire contracted period. .

7.10 Data Privacy

Data Privacy and Confidentiality

1. The bidder and respective OEMs shall maintain strict confidentiality of all Bank data, information, logs, reports, configurations, intellectual property, credentials, and other artifacts. Such information shall not be copied, accessed, processed, stored, transmitted, transferred, disclosed, published, or used outside the Bank's authorized environment or for any purpose other than execution of this contract without the Bank's prior written approval.
2. The bidder and respective OEMs shall comply with the Bank's Information Security, Cyber Security, Data Governance, Privacy, Data Retention, Digital Personal Data Protection (DPDP) Act, applicable regulatory requirements, and all other contractual obligations..

Executive Governance and Project Oversight

1. The bidder and each respective OEM shall nominate a senior executive as the Project Sponsor/Project Director responsible for executive governance, stakeholder management, escalation management, strategic oversight, and overall project success.
2. The Project Sponsor, Project Director, and designated senior representatives of the bidder and OEMs shall participate in governance meetings, executive reviews, strategy workshops, and escalation meetings as required by the Bank. An, On quarterly/or as per the frequency defined by bank, executive governance meetings shall be conducted throughout the contract period to review project progress, service delivery, operational performance, security posture, compliance, risks, technology enhancements, and continuous improvement opportunities.
3. The bidder and OEMs shall deploy and maintain adequately skilled, certified, experienced, and qualified resources, together with appropriate backup resources, succession planning, and skill development mechanisms, to ensure uninterrupted 24x7x365 service delivery throughout the contract period.
4. The bidder shall establish and maintain a Bank-approved Governance, Risk and Compliance (GRC) framework incorporating Key Performance Indicators (KPIs), Key Risk Indicators (KRIs), governance dashboards, and operational metrics for continuous monitoring of service quality, security, compliance, operational effectiveness, and project risks.
5. The bidder shall support the Bank's IT, Information Security, Cyber Security, governance, compliance, audit, regulatory, and technology transformation initiatives related to the scope of this RFP.
6. The bidder shall ensure that all deployed resources receive appropriate training on the proposed technologies, operational procedures, administration, troubleshooting, security operations, automation, analytics, risk management, and other functions necessary to perform their assigned responsibilities.

7.11 Warranty, ATS and AMC

Annual Maintenance Support (AMC) and Annual Technical Support (ATS)

1. The proposed hardware, appliances, shall include a comprehensive warranty of five (5) years commencing from the respective Go-Live date.
2. The bidder shall provide comprehensive onsite warranty and AMC for all hardware components and comprehensive ATS, subscription, and OEM support for all software, licenses, subscriptions, and services supplied under this RFP throughout the applicable contract period.
3. Warranty, AMC, and ATS services shall include OEM support, preventive and corrective maintenance, replacement of defective hardware, software updates, upgrades, patches, bug fixes, security updates, technical assistance, subscriptions, and all activities necessary to ensure secure, continuous, and compliant operation of the solution in accordance with the RFP and applicable Bank policies.
4. The rates quoted by the bidder for hardware, software, licenses, subscriptions, ATS, AMC, and related services shall remain applicable on a pro-rata basis for any additional quantities or services procured by the Bank during the contract period.
5. Installation of supplemental hardware by the Bank, with due intimation to the bidder and OEM, shall not invalidate or adversely affect the OEM warranty, ATS, or AMC applicable to the originally supplied hardware. Warranty, ATS, and AMC obligations shall not extend to such supplemental hardware unless procured under this contract.

7.12 Resource Requirement

The resource requirements specified in this RFP represent the minimum onsite deployment obligations. The bidder shall independently assess, size, and deploy additional onsite and offsite resources required to meet the implementation scope, service levels, project timelines, operational requirements, security requirements, and contractual obligations without any additional cost to the Bank.

7.12.1 Implementation Phase

- Prior to commencement of implementation, the bidder and respective OEMs shall submit a detailed Resource Deployment Plan for Bank approval identifying proposed onsite and offsite resources, roles, responsibilities, certifications, experience, deployment schedules, and solution-wise allocation.
- The bidder shall deploy a dedicated onsite Project Manager throughout the implementation phase and nominate appropriate bidder and OEM resources for each solution, workstream, milestone, and project activity.
- Any replacement, redeployment, or modification of approved implementation resources shall require prior written approval from the Bank.

7.12.2 Operations and Maintenance (O&M) Phase

- The bidder shall deploy the minimum onsite L1, L2, Project Manager/L3 – Operations, and other resources specified in the RFP and ensure uninterrupted 24x7x365 support through an appropriate shift-based deployment model.
- The respective OEMs shall provide subject matter experts from the date of installation throughout the contract period to support operations, troubleshooting, optimization, upgrades, audits, vulnerability remediation, and major incidents.
- The bidder shall ensure adequate SME support for timely resolution of incidents, service requests, problems, vulnerabilities, and operational issues.

7.12.3 Resource Management and Governance

- All deployed resources shall be named resources. The Bank reserves the right to interview, evaluate, approve, reject, or require replacement of any proposed resource before or during the contract period. Any resource found unsuitable, underperforming, non-compliant, or lacking the required competency shall be replaced by the bidder with an equivalent or better-qualified resource within the timeline prescribed by the Bank.
- Any replacement, withdrawal, reassignment, or removal of approved resources shall require prior written approval from the Bank.
- The bidder shall maintain adequate backup resources, succession planning, cross-training, and knowledge management practices to eliminate single points of dependency and ensure uninterrupted service delivery.

Resources may be deployed at the Bank's NextGEN SOC Office, Data Centre (DC), Disaster Recovery (DR) Site, SOC, or any other location specified by the Bank.

The Bank may require additional onsite resources during the contract period. Such resources shall be provided by the bidder at the pro-rata rates quoted in the Commercial Bill of Material, unless otherwise specified in the RFP.

The bidder shall remain solely responsible for ensuring adequate staffing levels and deployment of additional resources required to meet project timelines, operational requirements, service levels, and business continuity requirements throughout the contract period.

#	Resource Type	Deployment	Minimum Qualification & Experience
Implementation Phase			
1	Project Manager – Implementation	Onsite (Full Time)	• Graduate/B.E./B.Tech/MCA with PMP/PRINCE2 or equivalent certification. • Minimum 8 years of experience in SOC operations and management. • Experience in managing at least two SOC IT Security solution implementation and/or operations engagements in PSU/PSE/Government/BFSI/Regulatory organizations.
2	OEM Implementation Resources	Onsite (Full Time)	OEM shall submit a detailed resource deployment plan before commencement of requirement gathering. Any replacement or modification shall require prior Bank approval.
3	Bidder Implementation Resources	Onsite (Full Time)	Bidder shall submit a detailed resource deployment plan before commencement of requirement gathering. Any replacement or modification shall require prior Bank approval.
Operations & Maintenance (O&M) Phase			
4	L1 Security Resources	Onsite (Full Time)	• BCA/B.E./B.Tech/MCA with minimum 3 years of experience. • Minimum One OEM security certifications or equivalent certifications such as Cisco Certified Support Technician (CCST) Cybersecurity, CySA+, Security+, CEH Version 13 and above etc.

#	Resource Type	Deployment	Minimum Qualification & Experience
			• Experience in managing at least one SOC solution in PSU/ PSE/ Government/ BFSI/ Regulatory organizations/ Fortune 500 groups
5	L2 Security Resources	Onsite (Full Time)	• B.E./B.Tech/MCA with minimum 5 years of experience. • Minimum two OEM security certifications or equivalent certifications such as Azure/AWS Cloud certificate, CCSP, Cisco Certified Support Technician (CCST) Cybersecurity, SC-200, Security+ or equivalent. • Minimum 3 years in managing SOC • Experience in managing at least one SOC solution in PSU/ PSE/ Government/BFSI/Regulatory organizations/ Fortune 500 groups
6	L3/ Project Manager – Operations	Onsite (Full Time)	• B.E./B.Tech/MCA with "PMP/PRINCE2/ITIL/TOGAF or equivalent certification" and CISA/CISM/CISSP/CISSM/CCSP/OSCP/GIAC/GCSA/GPCS. • Minimum 8 years of experience in SOC operations and management out which minimum 5 years' experience as L3 or above in managing SOC. • Experience in managing at least two SOC solutions implementation and/or operations engagements in PSU/ PSE/ Government/ BFSI/ Regulatory organizations/Fortune 500 groups

The Bank reserves the right to interview, evaluate, approve, reject, or seek replacement of any proposed or deployed resource.

Before on boarding the resources, the Bank will conduct an interview round and if the resource found not competent the resource will not be on boarded.

The bidder is required to provide onsite human resource from the date of NextGEN SOC solutions installation.

The Bank may be required to increase onsite personnel resources of the bidder and / or OEMs from time to time.

The same need to be provided within one month from the date of such communication. The onsite resources must be provided adequate guidance, assistance and support by competent offsite subject matter experts (SME) of the bidder & OEMs

7.12.4 Minimum Resource Count Deployment

The following table represents the minimum mandatory onsite resources deployment requirements. The bidder shall right-size and deploy any additional resources as required to meet the SLA, operational, security, and business requirements defined in the RFP.

The Table below provides the minimal requirement to be positioned:

S. No.	Shifts	L1 (Minimum)	L2 (Minimum)	L3/ Project Manager (Minimum)
1	Shift A	4	2	1
2	Shift B	4	2	Bidder to right size
3	Shift C	4	1	Bidder to right size

Note:

1. The Above count is minimal Onsite personnel to the deployed by bidder 365 days in years.
2. Resources may be shared across technologies within the same domain, provided the minimum deployment requirements and SLA commitments are met.
3. The Bidder shall factor in adequate backup and replacement resources to ensure uninterrupted availability (24x7x365) of the minimum required number of on-premises resources, including during planned leave, unplanned absence, attrition, training, or any other contingency.
4. All resources deployed at the Bank's premises shall meet the minimum qualifications, certifications, skills, and relevant experience requirements specified in this RFP. The Bidder shall ensure that any replacement or backup resource also meets or exceeds the prescribed requirements for the respective role.
5. The bidder shall ensure availability of OEM specialists, architects, and SMEs for all proposed solutions throughout the contract period as and when required as per the requirements, scope of the RFP, and in line with the SLAs.
6. The bidder shall augment resources at no additional cost wherever required to meet service levels, incident response timelines, project milestones, or operational demands.
7. The above deployment represents the minimum mandatory onsite staffing requirement and shall not relieve the bidder of its responsibility to provide adequate resources for successful delivery of services.

7.12.5 Resource Deployment, Replacement and Governance

1. The bidder shall be responsible for meeting all SLA, operational, implementation, support, maintenance, and security requirements under the contract.
2. The Bank reserves the right to procure additional manpower from the bidder during the contract period on a pro-rata basis at the rates quoted in the Commercial Bill of Material.
3. Resources may be deployed at the Bank's NextGEN SOC Office, Data Centre (DC), Disaster Recovery (DR) Site, SOC, Branches, or any other location as specified by the Bank.
4. The proposed environment shall operate on a 24x7x365 basis. Accordingly, all deployed resources shall be capable of working in rotational shifts, extended hours, weekends, holidays, and during critical situations as required by the Bank.
5. The resource quantities specified in this RFP represent the minimum deployment requirements. The bidder shall appropriately right-size and augment onsite and offsite resources at no additional cost to ensure compliance with SLA, business continuity, operational, and security requirements.
6. All deployed resources shall be named resources. Any replacement, withdrawal, reassignment, or removal of a resource shall require prior written approval from the Bank.
7. In case of resource replacement, the bidder shall ensure an appropriate transition and knowledge transfer period as follows:
    - Project Manager/L3 (During Operations): Minimum 60 days
    - Key Personnel (L1/L2): Minimum 45 days
    - Other Personnel: Minimum 30 days
8. The Bank reserves the right to interview, evaluate, approve, reject, or seek replacement of any proposed or deployed resource. The bidder shall replace any resource found unsuitable, underperforming, non-compliant, or in violation of the Bank's policies within the timeline prescribed by the Bank. The non-availability of the resource will be considered a breach of the SLA. (Manpower Availability Clause)

9. The bidder shall ensure adequate backup resources, succession planning, cross-skilling, and knowledge management practices to eliminate single points of dependency and ensure uninterrupted service delivery.
10. During implementation, rollout, migration, critical incidents, audits, Go-Live, and other key project milestones, the bidder shall ensure active involvement and availability of senior management, project leadership, OEM representatives, and key technical resources.
11. All personnel deployed for the project shall carry valid bidder- or proposed Product OEM-issued identity cards at all times while performing services at the Bank's premises. The bidder and the proposed Product OEM shall provide the EPFO details of the deployed personnel to the Bank, as and when requested, for verification and compliance purposes. Subcontracting of any part of the services under this project shall not be permitted. The bidder's Authorized Signatory shall submit a monthly shift-wise deployment roster of all personnel with their names assigned to the project. Any changes to the roster or deployment schedule shall be communicated to the Bank in advance or, in exceptional circumstances, immediately upon such changes taking effect.

7.12.5.1 Responsibilities of L1, L2 & OEM Support

a. L1 SOC: Continuous monitoring of security events, initial alert validation, event triage, correlation review, identification of false positives, ticket creation, escalation of confirmed or suspected incidents and execution of documented standard operating procedures (SOPs).
b. L2 SOC: Detailed investigation and analysis of escalated incidents, advanced correlation and threat analysis, investigation across multiple data sources, incident containment and response support, root-cause analysis, threat hunting, tuning of detection use cases and coordination with L3 or OEM support wherever required.
c. OEM Support: Advanced technical investigation, product-level troubleshooting, complex incident response, malware and forensic analysis, platform engineering, advanced detection engineering, major use-case development, architecture-level changes and resolution of issues requiring OEM or specialist expertise.

7.12.5.2 Responsibilities of Project Manager/L3

The Project Manager/L3 shall, at a minimum:

a. Lead and govern the operational activities under the contract.
b. Act as the primary point of contact for the Bank's management and stakeholders.
c. Provide L3 technical support and advanced troubleshooting for complex, recurring, or unresolved incidents escalated by L1/L2 support teams.
d. Provide expert-level support for solution architecture, integration, configuration, performance tuning, and optimization of the proposed solution.
e. Review and validate L1/L2 troubleshooting and remediation activities and provide technical guidance
f. Provide technical inputs for service improvement, risk mitigation, and optimization of the deployed solution
g. Be accountable for successful delivery of the project and achievement of agreed timelines, milestones, and service levels.
h. Identify, track, escalate, and resolve project risks, issues, dependencies, and bottlenecks.
i. Coordinate with OEMs, service providers, Bank teams, and other stakeholders for successful delivery of services.
j. Monitor change management, deployment, migration, testing, and operational readiness activities.

k. Drive adoption of industry best practices, governance controls, and continuous improvement initiatives.

l. Submit periodic project status reports, governance reports, risk reports, and management updates to the Bank.

7.13 Facilities Management

1. Bidder should manage, monitor, maintain and upgrade all proposed solutions & services on ongoing basis encompassing all deployed hardware/ firmware/ middleware / software components by performing timely backups, continuous health monitoring, on-site and offsite support, troubleshooting, critical functional and performance bug fixes, all major product/feature enhancements within the warranty and AMC charges and as per the SLA defined by the Bank.
2. The Bidder shall ensure a considerable and measurable reduction in Mean Time to Detect (MTTD), Mean Time to Acknowledge (MTTAck), Mean Time to Assign (MTTA), and Mean Time to Respond/Resolve (MTTR) for security incidents by effectively leveraging the native capabilities of the deployed security technologies, SIEM, SOAR, automation, orchestration, and other relevant tools.
3. Bidder shall be responsible to develop and maintain Standard Operating Procedures (SOP) with respect to day to day operations including but not limited to threat management, alert/incident management, reports & dashboards, forensics infrastructure maintenance, rules creation & fine tuning, install/upgrades, updates, asset Integration, Business Continuity data & configuration backup, restoration, archival, knowledge management, segregation of duties, change management, patch & version management, KPI and KRI to measure performance etc. as per policies of the Bank. Bidder to create and modify SOP as per the requirement of the Bank periodically and from time to time, as applicable. All SOP will be reviewed by the Bank on monthly basis.
4. All onsite personnel resources of the bidder & OEMs should ensure to deliver the services leveraging security technologies as mentioned in the technology details, architecture and Terms & conditions in the bid, RFP, annexure, addendums, clarifications etc. issued by the Bank.
5. Bidder onsite personnel should be carrying out regular patch management, firmware updates, software upgrades, security updates, bug fixes, and configuration management of the deployed solution throughout the contract period. All critical, high-risk, and security-related patches/updates released by the OEM shall be assessed and applied in accordance with the Bank's change management procedures. The bidder shall proactively monitor OEM advisories and vulnerabilities and shall promptly implement necessary corrective actions to mitigate identified security risk.
   Minimum the table below should be compiled, which would be updated by bank and should be complied with by bidder:

Vulnerability Categorization	IT – AI-Exploitable Vulnerability	IT – Responsible Disclosure	OT – AI-Exploitable Vulnerability	OT – Responsible Disclosure
Critical	Emergency Release	7–15 Days	5 Days	15–30 Days
High	7 Days	15–30 Days	15 Days	15–30 Days
Medium	14 Days	30–60 Days	30 Days	

6. Every technology deployed should transform itself from a purely rule based system to analytics & AI/ML based correlation system for logs, vulnerabilities & threat intelligence together for accurate risks prediction.

7. To ensure efficient utilization and monitoring of proposed solution, optimizing capacity utilization, ensuring quality of data and system performance is maintained optimal, there are no security events omission, misfiring rules, heavy rules and reports etc.
8. Participate and contribute in every DR drill, cyber security drill, tabletop exercises by the Bank, regulators or any third party.
9. Conduct DR drill of the Security on quarterly interval or as and when required by the Bank. Ensure DC & DR are exact replica of each other in every manner.
10. Develop custom plug-ins, parsers, connectors, agents, adopters for all the systems in the Bank or related to the Bank periodically or as and when needed.
11. Develop the baseline for the level of logs to be enabled across the different components of IT including infrastructure, databases, business applications and devices etc. The log baselines should be in line with global best practices including NIST, SANS etc.
12. Perform monthly gap analysis of current levels of logs enabled in OS, databases, web servers, business applications and devices and entire IT infrastructure & recommend and implement remedial actions.
13. Install an agent-less model & rollout using an agent server for log collection wherever remote log collection is not feasible, bidder & respective OEM should work with the IT team to deploy the agent on the servers and applications.
14. Periodically assess the business requirements and configure the required rules, AI/ML based analytics models, self-learning models & processes and generate alerts as per the global best practices and Bank's requirements.
15. Securely preserve and maintain baseline repository of all the rules and models on analytical, self-learning, supervised & unsupervised learning and keep track of any changes / modifications.
16. Create new and customize existing reports, dashboards, rules, queries, user interface in all forms to meet the dynamic requirements of the Bank.
17. Define formats for MIS reporting that includes daily, weekly and monthly or any periodical or adhoc reports, dashboards as per the Bank's requirements.
18. Devise rules, AI/ML based models to analyse logs received from business applications to alert application owners about potential security threat / incident. OWASP and other threat modelling must be used for creating such rules, models. A minimum 15 unique use cases should be developed and implemented for each business application within first six months of go live date.
19. Transfer the knowledge to the Bank's employees about day-to-day operations, system / backend level troubleshooting, dashboarding, creating basic and advanced rules & analytical models, creation and customisation of reports &queries etc.
20. Complete system level frontend and backend management & maintenance related knowledge need to be transferred to the Bank's staff by the bidder's onsite L1 & L2 resources.
21. There should not be disruption or degradation in the Bank's network bandwidth utilization and availability due to excessive log transmission.
22. Conduct health check-up of the proposed systems by respective OEMs, refer section OEM Services & Deployment. The recommendations in the report should be rectified by L3 resources of respective OEM within a week's time. OEMs to ensure that their respective systems operate efficiently, cohesively without any adverse impact on processing, correlation, alerting, dashboarding etc. as per expectations of the Bank, stipulated in the RFP.
23. Secure configuration baseline should be benchmarked and updated on a periodic basis with standards including SANS, NIST, CIS, Bank's policies, CERT-IN, IDRBT, RBI guidelines as updated from time to time.

24. Bank provided IT Service Management (ITSM) or any other tool identified from time to time should be used for ticketing system, tracking instructions received from application / asset owners like integration, VA, PT, incident management etc. Instructions / actionable for day-to-day functioning within the team should also be routed through such tool. The entries in the tool should be able to provide jobs / activities completed, pending, pending at whose end etc. The performance & turnaround time / efficiency of onsite personnel resource would also be evaluated from the MIS generated from this tool.
25. All deliverables including reports, incidents / alerts, their closure, vulnerabilities reported and closed, dashboards, query optimization, indexing, automation based on AI/ML, backup & recovery activities etc. should undergo Quality Assurance process by resources of the bidder & respective OEM on ongoing basis. Project Manager should define quality metrics, measurement frequency and reporting periodicity in consultation with the Bank.
26. Ensure security of proposed setup from cyber-attacks & malwares etc. Any suspicious activity, behaviour of the proposed setup must be immediately taken into consideration and acted upon at the top priority.
27. For the security of the proposed setup, integrate the complete proposed setup with all the currently deployed tools and those procured from time to time.
28. For security monitoring of the proposed setup, integrate the complete proposed setup with SIEM, DAM, SOAR, TI etc. and ensure logs are auto sent to these tools by entire proposed setup on real-time basis on 24x7x365 days basis. These tools should automatically & immediately raise the alert to the designated official of the Bank, if no log is received for in 15 minutes initially. The duration will further be reduced from time to time.
29. Review onsite & offsite users as per Segregation of Duties (SoD) like their roles & responsibilities, access level / rights in the proposed technologies and other related onsite / offsite systems etc. on periodic basis and deactivate / modify user access etc. as per requirement with prior approval from the Bank.
30. Configuration and customization of the tools as per Bank's requirements on ongoing basis.
31. Feature requests, all critical, showstopper declared by the Bank needs to be implemented within 1 week including thorough functional, performance and security review. There should be no negative functional impact, data loss or performance degradation whatsoever with the introduction of new feature, enhancement, upgrade, bug fixes, customization.
32. Close every technical vulnerability in the proposed setup reported in vulnerability assessment (VA) within stipulated time i.e. critical/high risk vulnerability in prescribed timelines, medium/low risk vulnerability within the timelines from the date of reporting of such vulnerability/ observation.
33. Close every technical and non-technical vulnerability in proposed set-up other than VA such as vulnerabilities observed in internal or external audit / security reviews / SCD implementation, including but not limited to processes, techniques, SOP's etc. within stipulated time i.e. critical/high risk vulnerability in prescribed timelines, medium/low risk vulnerability in prescribed timelines from the date of reporting of such vulnerability / observation.
34. All the proposed solution must have latest encryption, hashing functions and PQC ready.
35. An automated workflow should be created and maintained for proposed solutions change management initiation, verification, approval, implementation and post-implementation verification.

36. Proposed solution should be compatible with IPv6 scheme, and there shall be no functional or performance impact on security monitoring due to switch over to IPv6 schema.
37. Monitoring of alarm conditions that are the result of correlation, pre-defined statistical violation (or baseline alarming) and other activity related to monitoring threat and inappropriate use cases.
38. Evaluate and analyse of a pattern that if viewed in isolation (each activity in isolation) would not constitute a threat, but in combination is an anomaly or a threat vector (e.g. statistical pattern defined).
39. Monitor, detect, prevent and appropriately respond against any known and unknowns' security threat, outliers, bots' identification etc.
40. Bidder/OEM must brief & provide executive summary, presentation before going for any major hardware/firmware/middleware/software version upgrade to cover all new features, functionality and bug fixes that are coming with new version/upgrade.
41. Bidder & OEMs should engage data scientists for analytics, statistical models, configuring the systems for supervised & unsupervised learning leveraging AI / ML to take over the activities of L1 & L2 resources by systems, minimizing the false positives and in developing advanced analytics use cases without any additional cost to the bank.
42. Bidder is responsible for overall project management, overseeing and addressing Bank's technical needs as & when arises to address critical and high severity issues.
43. Validation and signoff of delivered solutions / technologies, hardware & software configurations, vulnerabilities / security / hardening posture, services delivered as per the RFP.
44. At any of point of time during the project period of Contract period, if the performance of any system including cloud and related setup is found to be not satisfactory as per the Bank's expectation, then the Bidder and respective OEM shall be responsible to upgrade the hardware, software, applications etc. to meet the Bank's expectations at no extra cost to the Bank.
45. Bidder should ensure the proposed technologies, services are capable & configurable to send logs, data, network traffic, security alerts etc. on demand to regulators like CSITE, CERT-in, NCIIPC etc.
46. If any hardware, software, application, services has got additional component, feature, functionality, load bearing capability, domestic & foreign compliance requirements, security arrangement etc. which can be activated / provided in the proposed setup just by activating licenses and without procuring any hardware, then the same should be activated and provided in the proposed setup of the Bank without any extra cost to the bank.

7.13.1 Continual Improvement

1. Improve the policies configured on an ongoing basis to reduce the occurrence of false positives.
2. Periodic health checks should be carried out by the OEM to ensure the quality of implementation and operations.
3. Bidder shall curtail the closure time for incidents and events and ensure the periodic check-up reviews for the same.
4. Provide post go-live support, which includes but is not limited to system maintenance & support, system performance monitoring, system tuning, root cause analysis, change release management and day to day support, Solution maintenance, SLA compliance etc.
5. Provide support for the platform upgrades, customizations, configurations and resolving bugs/issues.

6. During the support period, the bidder will have to undertake comprehensive support of the platform and all new versions, releases, and updates for all standard product or specified software to be supplied to BANK at no additional cost. The Bidder shall maintain the platform to comply with parameters defined in this RFP.
7. Comprehensive maintenance shall include, among other things, day to day maintenance of the product or specified software a reloading of software, compliance to security requirements, etc. when required or in the event of system crash/malfunctioning, arranging, and configuring facility as per the requirements of BANK, fine tuning, system monitoring, log maintenance, etc. The services and the deliverables should strictly adhere to the SLAs.
8. Support would be comprehensive in nature and must have back-to-back support from the OEMs of the tools and CSP.
9. In the event of system break down or failures at any stage, following shall be specified:
    a. Diagnostics for identification of product or specified software failures and Root Cause Analysis (RCA)
    b. Protection of data/ configuration
    c. Recovery/ restart facility
    d. Backup of product or specified software / configuration
    e. The Bidder shall support the Software Solution, tools, and infrastructure provisioned during the entire contract duration as specified in Scope of work in this RFP.
10. The Bidder will be single point of contact and responsible for all, components, software, etc. The bidder must note that the managed services as a part of facilities management should be available for all environments viz., production, training, development, and test.
11. During contract period, the bidder will be responsible for:
    a. Overall maintenance and working of the solution.
    b. Bug fixing and delivery of patches/ version changes effected
    c. Providing tools for creating knowledge repository for the bugs identified, resolution mechanism, version upgrade, future upgrade etc. of Application software, tools, OS, RDBMS, application server software, web server software, interfaces, integrations, customization, reports etc.
    d. Provision should be available for version control and restoring the old versions if required by BANK
12. Bidder shall provide and implement enhancement/modification/patches/ upgrades/ updates for hardware/ software/ Operating System / Middleware etc. as and when released by Service Provider/ OEM or as per requirements of the Bank. Bidder should bring to notice of the Bank all releases/ version changes.
13. Configuration changes, performance monitoring, troubleshooting, patch installation, running of batch processes, database tuning, replacement / support, technical support, application, and data maintenance, taking backup of the database as required, recovery, query generation and management etc. of all software supplied under this RFP document.
14. Immediate bug fixing should be undertaken in the event of software failure causing an interruption of operation as per the response / resolution times defined by BANK. In case of any software /hardware /network failure, the solution should continue to function seamlessly.
15. All the detected software/hardware errors must be notified and corrected, as per the agreed timelines.
16. Support BANK in integrating any new applications to the proposed applications
17. Provide BCP/DR procedures and conduct DR drills in conjunction with BANK policies/procedures

18. Routing the transactions through backup system in case the primary system fails switching to the DR site in case of system failure
19. Service records and calls to helpdesk must be maintained and tracked for support, which will be reviewed monthly by BANK
20. Coordinating and scheduling maintenance activities with BANK and appropriate support functions of BANK/other providers (e.g., network support, facilities support, etc.)
21. Provide maintenance data, as reasonably requested by BANK, to support replacement / refresh scheduling.
22. Provide a single-point-of-contact to users for the resolution of problems.
23. Provide support and assistance, as required, to isolate complex network, operational and software problems related to the proposed solutions
24. Update, or provide the information required for BANK to update the asset management with BANK
25. Track and report observed Mean Time Between Failures (MTBF) for Hardware and Software
26. Release Control shall include the following but not limited to:
    a. All deliveries (full or patch) shall include a release note containing a full list of the contents of the delivery:
    b. Versions, file sizes and file modification dates of all components included in the delivery
    c. All reported faults which are newly fixed in the delivery, identified by fault reference code and including a brief description of the nature of the fix
    d. All change requests which are completed in the delivery, identified by the appropriate reference code, and including a brief description of the means whereby the change is implemented
    e. All information required to make any appropriate changes to the tuning and configuration of the production Systems or database such that they continue to meet their specifications
27. Provide assistance in IT Infrastructure Operations includes but not limited to:
    a. Major Incident Management
    b. Determining scope of the problem
    c. Managing the incident through service restoration
    d. Validating severity classification of the problem
    e. Facilitating Service Recovery Team meeting
    f. Escalating the issue as required
    g. Conducting Root Cause Analysis
    h. Preparing restoration plans
28. Compute Planning includes but not limited to
    a. Configuration Management
    b. Performance Management
    c. Capacity Management
29. Provide problem escalation and interact as necessary with third party suppliers.
30. Provide monitoring and troubleshooting for the entire in-scope solutions & services.
31. Provide timely notification and escalation to onsite personnel if any hardware and software conditions exist that must be resolved on site to meet the service levels provided in this schedule.
32. Monitor the status of system processes and events.
33. Monitor and respond to system alerts and event.
34. Monitor and maintain system error logs.

35. Perform application, database, storage replication across the DC & DR as per required Service Levels.
36. Shifting of IT hardware within the premises, reinstallation and configurations including cabling and asset labelling.
37. Asist in executing the backup and recovery procedures.

Note: BANK will not be liable to pay any additional charges in respect of any sort of maintenance required during the tenure of the contract.

The list of activities mentioned below are indicative, bidder is required to perform all the activities not limited to the one mentioned in the RFP for maintenance, management and successfully meeting the terms of the RFP.

7.14 DR Drill

The bidder is responsible for conducting the DR Drill on a regular basis and as per the frequency decided by the bank in the presence of bank officials. Coordination with the application team, OEMs and bank's team, is the responsibility of the bidder to ensure the successful execution of the DR drill. The bidder is required to maintain documentation of the DR Drill and provide suggestions on improving the RTO and RPO of DR drills. The DR Drill report with learnings, outcome of the drill must be submitted to the Bank and same will be subject to the audit by the Bank. The periodic DR Drill plan should be submitted in advance to the bank for scheduling the same in presence and approval of the bank.

7.15 NextGEN SOC operations:

Bidder is responsible for below operational matters during the Contract period.

1. The bidder should manage, monitor, maintain and upgrade all NextGEN SOC solutions on ongoing basis encompassing all deployed hardware / firmware / middleware / software components by performing timely backups, continuous health monitoring, on-site and offsite support, troubleshooting, critical functional and performance bug fixes, all major product/feature enhancements within the warranty and AMC/ATS charges and as per the SLA defined by the Bank for Contract period.
2. All onsite resources should ensure to deliver the services leveraging NextGEN SOC technologies as mentioned in the technology details, architecture and Terms & conditions in the RFP, addendums, corrigendum, clarifications etc. issued by the Bank.
3. The onsite resources must be provided with adequate guidance, assistance & support by competent offsite subject matter experts (SME) of the bidder & OEMs.
4. Bidder to ensure efficient utilization and monitoring of Licenses, optimizing capacity utilization, ensuring quality of data and system performance is maintained optimal, there are no security events omission, misfiring rules, heavy rules and reports etc.
5. Participate and contribute to every DR drill, cyber security drill, table-top exercises by the Bank, regulators or any third party.
6. Conduct DR drill of the NextGEN SOC on quarterly interval or as and when required by the Bank.
7. Develop custom plug-ins, parsers, connectors, agents, adopters for all the systems in the Bank or related to the Bank periodically or as and when needed without any extra cost to bank.
8. Develop the baseline for the level of logs to be enabled across the different components of IT including infrastructure, databases, business applications and devices etc. The log baselines should be in line with global best practices including NIST, SANS etc. followed by govt., regulatory compliances, Cybersecurity framework and ISO 27001:2022.
9. Perform fortnightly & monthly gap analysis of issues/threat/vulnerabilities in OS, databases, web servers, applications and devices and entire IT infrastructure & recommend and implement remedial actions.

10. Periodically assess the business requirements and configure the required rules, AI/ML based analytics models, self-learning models & processes and generate alerts as per the global best practices and Bank's requirements.
11. Creating new reports and customize existing reports, dashboards, rules, queries, user interface in all forms to meet the dynamic requirements of the Bank.
12. Define formats for MIS reporting that include daily, weekly and monthly or any periodical or ad-hoc reports, dashboards as per the Bank's requirements.
13. There should be alert generated and sent to concerned owner(s) for every Potential Security Threat and Incident identified based on the configured rules, and comprehensive AI/ML based modelling on the logs received from the respective Application(s). This mechanism should be based on OWASP foundation and other leading threat modelling Parameters based on the best practices. Unique use cases should be developed and implemented for each business application.
14. The bidder shall perform end-to-end investigation of security alerts and incidents, including triage, enrichment, correlation, scoping, impact assessment, root-cause analysis, containment/response coordination, recovery validation and closure, with appropriate investigation records and supporting evidence maintained in the designated systems.
15. The bidder shall continuously assess and enhance NextGEN SOC detection and response capabilities for emerging AI-enabled and AI-assisted cyber threats, including AI-generated phishing and social engineering, automated attacks, adversarial use of AI, abuse of AI/GenAI applications and services, and anomalous use of AI services, based on available telemetry and the Bank's risk profile.
16. Transfer the knowledge to the Bank's IT employees and/or Banks' NextGEN SOC team about day-to-day operations, system / backend level troubleshooting, dashboarding, creating basic and advanced rules & analytical models, creation and customization of reports &queries etc.
17. There should not be any disruption or degradation in the Bank's network bandwidth utilization and availability due to excessive log transmission or any configurations/customization in the proposed solution.
18. Secure configuration baseline should be benchmarked and updated on a periodic basis with standards including SANS, NIST, CIS etc. followed by Bank's policies, CERT-IN, IDRBT, RBI guidelines as updated from time to time.
19. The bidder should use bank provided Ticketing tool identified from time to time for ticketing system, tracking instructions received from application/asset owners like integration, VAPT, incident management etc. Instruction/actionable for the day-to-day operation within the NextGEN SOC team should be routed through such tool. Such entries in the ticketing tool should be able to provide activities/jobs completed, pending, pending at which/whose end etc. The performance & turnaround time/efficiency of onsite personnel resource would also be evaluated from the MIS generated from this tool/system.
20. All deliverables including reports, incidents/alerts, their closure, vulnerabilities reported and closed, dashboards, query optimization, indexing, automation based on AI/ML, backup & recovery activities etc. should undergo Quality Assurance process by the onsite resources on an ongoing basis. Project Manager of the bidder and Bidder should define quality metrics, measurement frequency and reporting periodicity in consultation with the Bank.
21. Bidder to ensure security of NextGEN SOC setup from cyber-attacks & malwares etc. Any suspicious activity, behaviour of the NextGEN SOC setup must be immediately taken into consideration and acted upon at the top priority.

22. For the security of the NextGEN SOC setup, bidder should integrate the complete NextGEN SOC setup with all the currently & to-be deployed tools and those procured from time to time by the bank.
23. The successful bidder should provide comprehensive AMC & ATS for proposed solutions, including other software, associated modules, hardware and services required to meet the requirements in the RFP.
    a) The AMC/ATS support for the complete solution should include the following:
    b) All version upgrades (as per the functionalities and features asked in RFP including the observations raised during VAPT/RBI) during the period of contract at no extra cost.
    c) Program updates, patches, fixes and critical security alerts as required.
    d) Documentation updates.
    e) 24*7*365 support for all the security application related malfunctions and ability to log requests online.
    f) The Bidder should have back-to-back agreement with the OEMs for ATS and AMC support.

Application management includes but not limited to:

Task	Activities
Services required	1. Installation, configuration, and Un-installation of application 2. Processing Change requests 3. Bug fixing & patch management 4. Vulnerability Assessment and management 5. Data Migration and Uploading 6. Application code migration to new environment 7. Incident and problem management 8. 24*7 Performance Monitoring & Management of application 9. Application Patch management and version control 10. Secondary site setup creation and DR management including DR synchronization, DR drill, etc. 11. Perform Primary – secondary site drills (DC-DR Drills) 12. Managing capacity and augmenting in order to meet the SLAs 13. Deploying objects in Application server 14. Troubleshooting Application server product related issues and Patch Management 15. Configure, start, stop, and manage Server services for all environment and nodes as required. 16. Configure and manage HTTP/HTTPs 17. Configure and use monitoring tools provided for Application Server 18. Backup & restoration management of application server 19. Performance management 20. Vendor management (Logging a call with product Vendor) 21. Version migration, testing and implementation 22. File Level Backup of compute 23. Portal/content management. 24. User management 25. Support to known errors and problems 26. Monitor web / Application server availability

Task	Activities
	27. Monitor alert notifications, checking for impending problems, triggering appropriate actions. 28. Bidder is required to factor in a solution to automate the batch jobs to meet the requirements of the RFP.

24. OS/Server/Appliance/Hardware Management categorized under Incident, Problem and performance Management Services
    a. Bidder needs to provide below mentioned services but should not limit itself to this list:
        i. Account administration and access management within the proposed security solutions.
        ii. Performance monitoring, incident management, and problem management for the proposed security solutions.
        iii. Monthly and fortnightly incident, event, alert, and service analysis.
        iv. User rights, role, and privilege administration within the proposed security solutions.
        v. Monitoring solution availability, service health, integrations, log collection status, processing performance, storage utilization, database growth, and application performance.
        vi. Preparation of preventive maintenance schedules, health check reports, capacity utilization reports, and root cause analysis reports for the proposed solutions.
        vii. Implementation and validation of application patches, hotfixes, signatures, threat intelligence updates, content updates, and security updates released by the respective OEMs.
        viii. Security hardening and secure configuration management of the proposed security solutions.
        ix. Troubleshooting alerts, incidents, errors, and performance issues related to the proposed security solutions.
        x. Incident resolution, tracking, escalation, and closure.
        xi. Participation in DC-DR failover, restoration, and business continuity testing activities related to the proposed security solutions.
        xii. Coordination and escalation with OEMs, infrastructure teams, cloud service providers, and other vendors as required.
        xiii. Review and audit of privileged accounts, administrative activities, logs, and audit trails within the proposed security solutions.
        xiv. Validation of backup, restoration, archival, and recovery activities related to configurations, policies, rules, use cases, dashboards, reports, and solution databases.
        xv. Log monitoring, analysis, correlation, retention, archival, and lifecycle management.
        xvi. Restoration and recovery drills for the proposed security solutions.
        xvii. Definition of backup requirements, validation of backup schedules, and coordination for resolution of backup failures with the respective infrastructure teams.
        xviii. Performance tuning, optimization, and capacity planning of the proposed security solutions.

Note: *Bidder is also expected to offer any other service that is required for the above purposes and is not mentioned in the list.*

7.16 OEM Services & Deployment (Architecture Assessment):

Assessment & performance review

1. Review of respective solutions configurations (Custom parsers, playbooks, controls, rules and process etc.) of the OEM solution
2. System Optimization review and suggestion including remedial actions.
3. Review the bidder's implementation of suggestions of remedial actions.
4. List of Solution for which Assessment is to be conducted, Year 2 Onwards are:

Solution	Frequency
SIEM	Year 2- Half yearly Year 3- Half yearly Year 4- Yearly Year 5- Yearly
SOAR	Year 2- Half yearly Year 3- Half yearly Year 4- Yearly Year 5- Yearly
UEBA	Year 2- Yearly Year 3- Yearly Year 4- Yearly Year 5- Yearly
XDR	Year 2- Yearly Year 3- Yearly Year 4- Yearly Year 5- Yearly

5. Incident Handling and OEM Involvement:
   a) For any concerns, incidents, issues or identified threats/vulnerabilities etc.—especially those classified as critical —the bidder is required to engage with the respective OEMs at regular intervals to ensure timely and effective resolution.
   b) Furthermore, any resolution proposed or implemented by the bidder for a critical-level incident must be reviewed and formally certified by the respective solution's OEM ensuring that the resolution aligns with OEM best practices, maintains system integrity, and does not introduce new risks or vulnerabilities.
   c) Regular collaboration with OEMs should also include proactive reviews, patch advisories, configuration validation, and support for root cause analysis, where applicable.

7.17 System recovery

1. In case of disaster, it is the responsibility of the Respective solution OEM along with the bidder to ensure that services remain unaffected and same is up and running from secondary site (DR)
2. It is bidder's responsibility to maintain DC – DR patches, updates & upgrades on continuous basis. Bidder to ensure that scheduled / unscheduled DR drills is conducted on regular basis (Quarterly basis or as defined by BANK). As part of these exercises, bidder to submit compliance / completion of activity reports at the end of the activity.
3. Bidder is responsible for performing DR drills between the proposed primary (DC) & secondary site (DR). Also, bidder to participate and assist BANK in their DR drill (planned & unplanned) and ensure the availability of solution during BANK's drills. During the DR Drills, bidder to ensure that full manpower deployment is made available during the drill.
4. Processes shall be in place to allow for recovery to a disaster recovery hardware platform, and the bidder shall provide Estimates of recovery time.

5. Proposed method of recovering the logical state of the production service, Likely extent of data loss in the event of such recovery being required
6. The Bidder shall maintain following documentation and same shall be shared during the start of the project and every MONTH highlighting the updates made in the document with respect to the previous version.
   a) Disaster Recovery Plan- identifying the operations involved in disaster recovery and the dependencies between these operations.
   b) Disaster Recovery Procedures- providing step-by-step instructions for the operations identified in the Disaster Recovery Plan
   c) Disaster Recovery Test Plan- identifying the steps and resources required to carry out a Disaster Recovery test to validate the Disaster Recovery Plan and Procedures
7. The Bidder shall ensure that each batch job (if any) can, following a failure, be restarted from the point of failure once the cause of the failure has been removed

7.18 IT Infrastructure requirements

1. Bidders must design, size, supply, commission, maintain and manage suitable and required hardware infrastructure for the proposed solutions in the RFP response at the location specified in the RFP (DC and DR). Bidder should size hardware based on the volumes mentioned in Annexure 21: Volumetrics of this RFP at relevant locations- DC, DRC and branches.
2. If the proposed solution is cloud-based, the bidder must accurately right-size the cloud infrastructure to meet all performance, capacity, and SLA requirements outlined in the RFP. The design should ensure availability within the primary cloud site, incorporating failovers, backups, and health monitoring, while also including a disaster recovery plan with a secondary site that meets the defined requirement as stated in the RFP. The proposal should include detailed architecture diagrams and a sizing justification.
3. The proposed IT Infrastructure/Hardware Appliances model should not be end of sale product at the time of bid submission, and supportability (End of Life or End of support) of the product should be available for the entire contract period. Bidder to submit the undertaking on OEM's letterhead as per Annexure 26: Undertaking – Support & Launch Confirmation.
4. The proposed architecture shall ensure appropriate availability and failover within the primary cloud environment, applicable backup and health-monitoring capabilities, and disaster recovery through the required secondary site/DR architecture in accordance with the requirements specified in this RFP.
5. The Bidder shall submit detailed architecture diagrams and sizing justification for the proposed cloud/hybrid infrastructure.
6. Bidder should arrive at the sizing independently along with the respective OEMs. In case, the sizing quoted by the Bidder fails to meet the necessary services, SLA and other terms of the RFP, bank will not bear any cost for upgrades or replacements. Also, during the contract period, growth of the bank should be considered and thus, the appliances, solution, IT Infrastructure proposed should have enough CPUs, memory, storage, NIC, Ports, etc. available to accommodate the predicted sizing, SLAs and other requirements of the bank as required. The appliance/devices/cloud environment proposed must have adequate vertical headroom. Any additional cost required for horizontal scaling would be borne by the Bidder in case of breach/ SLA bottleneck.
7. Bidder is required to propose a system which includes the OS, Database, compute nodes, storage system, network system, Backup Infrastructure & Solutions etc.
8. Bidder is required to provide staggered hardware, associated software and applications depending on the volumetric defined in the RFP. The subsequent AMC/ATS of the components will begin as per the phased delivery.
9. All hardware (Production, Non-production, and related hardware components) and system software components required for the project, must be included in the bill of Material of the bidder. In case the bidder fails to do so, and the project demands additional components at a later stage, then the bidder will have to provide additional components at no additional cost to the bank. DB audit trails should be enabled across all environments, and bidder is required to size the hardware accordingly.
10. Necessary services over and above this, such as implementation, management, SLA etc. will be the sole Responsibility of Bidder. The PSB expects Bidders to optimally size and factor the requirements in compliance with the RFP requirements. However, if at the time of implementation there is a shortfall/non-compliance of any component/hardware/software required for the functioning of Bidder's proposed

solutions with respect to the proposed hardware/software, Bidder will be required to provide additional hardware/software at no additional cost to the PSB.

11. Bidder shall install and commission the required IT hardware assets and software components into the racks to build the required setup.
12. Bidder shall be responsible for providing all the logs and required telemetry data for the setup and ensuring its integration with the centralized SOC of PSB.
13. Bidder shall position a dedicated technical onsite team consisting of L1, L2 and L3 resources to implement, commission and manage the proposed set-up in managed services model in accordance with the necessary security policies and guidelines issued by GOI/MoD/MietY/Other regulatory & statutory body from time to time.
14. The bidder shall ensure that the SoPs, procedure, policies and guidelines etc. for the proposed infrastructure & solution must be fully compliant with the latest certification requirements of ISO 20000, ISO 27001, ISO 22301, ISO 27701, ISO 27017 etc. During the contract, if PSB/PSB appointed agencies identifies any shortcoming/ lack of compliance, the bidder shall be responsible to ensure compliance.
15. The bidder shall provision all the required hardware, software, licenses and other components required for the setting up of this management cluster and also ensure the availability of solutions as per the defined SLAs.
16. Entire solution (hardware & software) should be IPv6 implementation ready from day one, considering IPv6 security practices.
17. Bidder to propose and factor the quantities required for any overhead for running the overall solution such as the orchestration, virtualization solution, containerization, or any other component as required.
18. Bidder can consider logical separation/ Virtualization for production and non-production environment at compute and storage level for respective Environments. The bidder should note that the production and non-production environment should be physically separate with respect to Compute. Bidder is required to consider and propose SAN Switch, Backup Solution (Backup Software, Backup Server, long term storage, D2D) which can be used both for production and non-production environment logical separation / Virtualization / zoning.
19. Production Environment:
    a) The virtualization should be implemented in such a way so that there is no single point of failure, in case of one instance / node is deployed in server 1 then the second instance / node of the same environment of the solution should not be deployed in the same physical server.
    b) Example: Assuming the proposed solution requires two web nodes say Web01 and Web02 and have three Production servers SRVPRD01, SRVPRD02 and SRVPRD03 with virtualization implemented; if Web01 node is deployed in SRVPRD01, then Web02 node is not allowed to be configured in SRVPRD01, it is to be configured either in SRVPRD02 or SRVPRD03.
    c) The Web Application can be virtualized to provide flexibility and scalability; however, it is important to note that the Web and Application tiers will reside in separate VLANs to enforce network segmentation and security. All east-west traffic between these VLANs will pass through a firewall to control and monitor inter-tier communication, ensuring strict access policies and reducing the attack surface. The architecture should be designed accordingly to support this layered security model.

d) The Database server will be deployed on a completely separate physical or virtual infrastructure, isolated from both the Web and Application layers, to further enhance security, performance, and fault isolation across the entire system.

20. Bidder shall provide legally valid Software/ hardware/ firmware Solution. The detailed information on license count and type of license shall also be provided to the Bank.
21. The bidder is responsible to provide the correct sizing of compute, network, and storage, IOPS including server etc. in collaboration with the proposed OEM whose solution/technologies are proposed for Nextgen SOC for successful deployment. Bidder and OEM should also account for scalability and future growth of the Bank to arrive at sizing for the Contract period.
22. In the event of failure, the system should automatically initiate failover within seconds, ensuring uninterrupted functionality without requiring manual intervention. The failover shall be completed within the applicable RTO/SLA (Section 13) requirement specified in this RFP, while maintaining the required service availability and functionality.
23. All hardware and software components should be architected for seamless scalability at DC & DR, ensuring long-term capacity.
24. Each node/environment must be individually provisioned for full peak load

7.18.1 Compute Infrastructure

1. Bidders must design, size, supply, implement, maintain and manage suitable compute infrastructure for all the in-scope applications/solutions proposed in the RFP response.
2. The hardware sized should be redundant, both horizontally and vertically scalable, fault tolerant and designed for high availability.
3. Bidder has to provide the similar category (i.e., mainly same class - similar processor and OS platform) of servers for Test, Development and Training Environment as that of the proposed production.
4. Vertical and horizontal scalability should be two important requirements for the servers as well. Bidder should arrive at the sizing independently keeping growth roadmap in consideration.
5. Ensure servers include sufficient CPU cores, RAM, and network interface cards (NICs) to handle expected transaction volumes, data processing needs, parallel operation of Backup & Restoration (with Ransomware Protection) and Replication.
6. Proposed hardware should have separate FC/LAN Cards enabling separate subnet creation for backup process, if required.
7. The virtualization architecture must ensure no single point of failure. In case of one instance / node is deployed on server 1 then the second instance / node of the same environment of the solution should not be deployed in the same physical server.
8. The production and non-production environment should be separated to meet the requirement of the bank.
9. Production Environment:
    a) There will be separate virtual machines for Web Server, Application Server, and Database Server etc. All are in different logical zones separated through firewall to communicate with each other. Accordingly, the connectivity should be established to make them operational. In no case will communication be permitted without firewall and / or IPS. Bidder must ensure the communication in the desired way and all the required hardware, software and network equipment(s) etc., if required will be provided by bidder only.
10. Necessary Hardware, Software and Services over and above this, such as implementation, SLA etc., will be the sole Responsibility of the Managed Service Provider/OEM. Managed

Service Provider/OEMs to optimally size and factor the requirements in compliance with the RFP requirements. However, if at the time of implementation there is a shortfall/non-compliance of any component/hardware/software required for the functioning of the Managed Service Provider/OEM's proposed solutions with respect to the proposed hardware/software, Bidder will be required to provide additional hardware at no additional cost to the Bank.

11. The bidder is required to factor in the necessary compute resources for analytics, AI/ML modeling, etc., and include these details as part of the Bill of Quantities (BOQ).

7.18.2 Storage Infrastructure – Primary

1. Bidder will be responsible to design, size, supply implement and manage the Storage Solution in compliance with the RFP requirements at DC and DR.
2. Supply, installation and implementation of storage hardware (Primary), including SAN systems, with adequate capacity and IOPS (Input/Output Operations Per Second) as per requirements.
3. Bidder will be responsible for the comprehensive end to end design solution of the Storage across the sites which should include Minimal Data Loss, Replication and any other requirements stated in the RFP that relate to the storage.
4. Any component/software/service required by Bidder that does not fall under the existing Storage requirements must be factored by Bidder.

7.18.3 Backup Infrastructure

1. Bidder is required to size, design, supply, implement and manage the Backup Software along with necessary hardware (including backup storage) as part of the assignment.
2. Bidder to factor the required solution and infrastructure to ensure taking and securing backup as per the PSB policy (which will be updated from time to time). The sizing of the Backup solution has to be determined by Bidder in accordance with the storage sizing.
3. The bidder should configure, schedule and manage backups of all the data including but not limited to files, folders, images, system state, databases and enterprise applications as per the policy defined by PSB.
4. The scope of work also includes backup replication to DR Site.
5. Bidder must provide Backup solutions (on-prem solution with cloud ready capabilities) including required hardware, storage, software, and licenses for performing automated backups of configurations and data for NextGen SOC solutions. The bidder should also ensure that sufficient storage is factored in during the contract period.
6. Backup & restoration solutions should be made by the team deployed by bidder aligning with the requirement mentioned in the Annexure 21: Sizing/Volumetric
7. The bidder should be able to make the required modification in backup procedures as per PSB at no additional cost to PSB.
8. In case any security application/tool is proposed on Cloud (SaaS) or Hybrid deployment, the Bidder shall ensure appropriate backup of the proposed security solution, including applicable configuration, operational data, logs, audit trails and other Bank-owned information, in accordance with the applicable backup, data-retention, security, data-residency and DR requirements of this RFP. The Bidder shall provide/restore such backup data to the Bank as and when required by the Bank, subject to applicable security controls and access procedures.

7.18.4 Networking and Security Equipment:

1. Ensure network equipment is compatible with existing infrastructure and configured to optimize security, speed, and reliability.
2. Specify quality of service (QoS) settings, VLANs, and any necessary configuration protocols to ensure seamless data flow and security.

7.18.5 Software

1. Bidder should propose Enterprise/OEM Supported based licenses and must issue in the name of PSB. Only supported and stable version of solution can be considered for the proposed systems. The proposed solution should be the latest and stable version.
2. The bank will be entitled to use the new product features, upgrades, device models, new versions etc. without any additional cost to the bank.
3. Enhancement/ upgrades/ updates/fixes/patches/functionalities/subscriptions for hardware/ software/ Operating System / Middleware etc. should be implemented, post approval from bank, in the bank environment as and when released by Service Provider/ OEM or as per requirements of the Bank
4. Functionalities, features, and components forming part of the Bidder's proposed solution at contract award shall remain available to the Bank at no additional cost for the Contract Period..
5. No committed functionality or SLA shall be withdrawn or restricted during the Contract Period due to OEM roadmap or licensing changes, except where the OEM discontinues the capability entirely
6. If the OEM discontinues or materially alters a proposed functionality, the Bidder shall provide a functionally equivalent replacement at no additional cost, without adverse impact to SLA-committed performance.
7. New features and upgrades released by the OEM during the Contract Period, to the extent applicable to the proposed solution and sought functionalities &scope, shall be made available to the Bank at no additional cost, subject to the Bank's change-management approval.

7.19 Other In-Scope Services

7.19.1 Other Scope Activity

1. The Respective solution OEM along with the bidder is expected to ensure that all functionalities as mentioned in Appendix 1A: Functional Specification are made available to PSB.
2. The Respective solution OEM along with the bidder is expected to ensure that for the purpose of this RFP, statutory and regulatory changes shall mean any change prescribed by the statutory and regulatory bodies governing/ affecting the banking industry in India viz. Reserve Bank of India, Ministry of Finance, CCIL, NPCI, IBA, SEBI, or any such bodies constituted by the RBI mandating change/s to an existing functionality of the Solution shall be provided to the Bank at no additional cost for the entire contract period. However, any Statutory and Regulatory changes post Go-Live of the respective applications (which are not a part of the existing functionalities) will be on CR basis based on the rates provided in the Bill of Material.
3. The Respective Solution OEM along with the bidder is expected to carry out a requirement study for the functionalities and services required by PSB, to gain understanding of the business requirements.
4. Respective solution OEM along with the bidder must note that it shall not be permitted to change the proposed OEM Solution after submission of bid. Bidder must also note

that it shall not be permitted to quote any options of solution/OEM. Failure to adhere to this clause may attract disqualification of the bid / contract as well as invoke related damage clauses as specified in Terms and Conditions.

5. The Respective Solution OEM along with the bidder is expected to customize the screens, design and layout of the solution depending on the requirements of the bank, at no additional cost to the bank as per the specific UI/UX design finalized during the SRS
6. The Respective solution OEM along with the bidder is expected to customize the solution based on the requirements of bank.
7. The Respective solution OEM along with the bidder is expected to support the bank in the installation, implementation, rollout and maintenance of all the proposed applications.
8. The Respective solution OEM along with the bidder is responsible to impart requisite training to the bank officials as per the ask of the RFP
9. The Respective solution OEM along with the bidder has to ensure the seamless switching of all the services to Disaster Recovery (DR) site during DR drill as and when decided by Bank or in case of non- availability of primary/ DC site.
10. The Respective Solution OEM along with the bidder needs to mention any other security feature supported by the system with details and architecture of the security components.
11. The Respective solution OEM along with the bidder is required to make changes in the Solution including software, procedure and operations as required by regulators from time to time to comply with any new rules of Indian Law, RBI, IBA, TRAI, Govt. of India, NPCI guidelines and other Regulator body for all the Proposed Solutions.
12. The Bidder should ensure continual security of the software/solution. Any development activity for incorporating security measures should be a part of the ATS.
13. The hosting Space and Power arrangement shall be provided by the Bank at DC and DRC. However, the bidder is required to factor in the requisite racks in order to successfully operationalize the proposed hardware.
14. It is the responsibility of the Respective Solution OEM along with the bidder to resolve any deficiency identified in the performance of Proposed Solutions, as observed during the acceptance test. This includes replacement of some or all equipment at no additional cost to the Bank, to ensure that the solution meets the requirements of the Bank as envisaged in the RFP.
15. The Respective solution OEM along with the bidder shall ensure that all functionalities, features, capabilities, modules, connectors and integrations included in or committed as part of the proposed Solution at the time of Bid submission / Contract Award shall remain available to the Bank throughout the contract period at no additional cost, notwithstanding any subsequent change by the OEM in its licensing model, subscription model, product edition, SKU structure, feature bundling or pricing model. Where any such committed functionality is subsequently moved to a separately chargeable module, restricted to a higher tier, or withdrawn, the Bidder/OEM shall provide the same or an equivalent capability at no additional cost to the Bank for the remaining contract period.

7.19.2 Transition Management

1. The Bank shall provide the Selected Bidder complete details of the existing security infrastructure, deployed solutions, architecture diagrams, inventory, integrations, licenses, OEM support contracts, operational procedures, and incumbent vendor support arrangements as available with the bank during the project initiation period.
2. The Bidder shall take over and maintain the operations and support of the Bank's existing solutions with effect from 01.05.2027, on an “as-is and where-is” basis, and

shall continue to provide uninterrupted operations and support until the proposed/new solution is successfully implemented, commissioned, and goes live, in accordance with the requirements of this RFP.

3. The Bidder shall deploy the required qualified and experienced support resources at the Bank's premises with effect from 01.05.2027 to perform the day-to-day operations, monitoring, administration, troubleshooting, maintenance, incident management, and support of the existing solutions. The "as-is and where-is" basis shall not exempt the Bidder from meeting the applicable SLAs or from any consequences arising from a breach of such SLAs.
4. The bidder shall run the existing SIEM on as-is/where-s basis for another 12 months from the date of Go-Live of the respective solutions.
5. The Bank shall enable adequate cooperation and knowledge transfer support from the incumbent service provider(s). However, it is the responsibility of the bidder to liaison with the existing vendors and the OEMs.

7.19.3 Security Management

1. Authentication and authorization mechanism for all users and systems should ensure enforcing bank's security policies.
2. End to end security mechanism to ensure security of logs, data, information, alerts, users, configurations etc. at rest / storage / database, during processing and in transit.
3. User id and login should determine level of access to data e.g. read/view data, print data, write/modify data, delete data etc.
4. The solution should support the following security features:
    a) Username and password for accessing the applications and database
    b) Access credentials should not be stored on the endpoints
    c) Auto blocking/locking of applications access upon reaching maximum number of tries. The maximum number of incorrect errors should be defined by the Bank
5. Termination of session and log off after lapses of configurable time period.
6. The solution should support the following transaction level security:
    a) End-to-End encryption of data transmission (symmetric or asymmetric)
    b) The solution should support multiple authentication-based bank's preferences
7. The solution should support the following platform security & reliability:
    a) Data stored is encrypted in the platform database
    b) Audit trails and logging features must be available in Web Server, application server and database server
    c) Ability to assign specific rights to platform administrators for secure and restricted access
    d) Solution should have the ability to support external certifying authority
    e) The solution should have secure interfaces to various hosts systems according to prevailing security standards
    f) Application access credentials should not be stored locally.
    g) Solution should support standard algorithms like AES
    h) Solution should have a minimum encryption strength of 256 bit for end-to-end transaction (Standard encryption algorithms like 3DES, AES, PKI scheme, with minimum encryption strength of 256 bit)
    i) The predefined pages of the web portal should handle web application security threats like Cross-site scripting, SQL injection flaws, Malicious file execution, Information leakage, Improper error handling, Broken authentication and session management, Insecure Cryptographic storage, Failure to restrict URL access.

j) Platform should have a clear separation of security responsibilities and should be designed for externalized security implementing JAAS (Java Authentication and Authorization Services) allows for pluggable providers
k) OWASP Top 10 Compliant
l) Password must be hashed by SHA256 at least and include Salt or using salt supported cryptography
m) All the sensitive data (e.g. passwords), including their backups, stored in an encoded or encrypted form in order not to be readable in case of exploitation or other application corruption
n) Sensitive Data Exposure:
    i Sensitive data should be masked when output.
    ii Sensitive data should not be stored in source code, config files and logs.
    iii Passwords are hashed using Salt.
o) Configurable approval rules set up for Bank administrator to perform the actions
p) Regulatory & Statuary
    i The solution should comply with the security principles and practices as stipulated by Statuary and regulatory authorities in India
q) Application
    i OS Security check up. Application should have capability to detect if the application is running on a jail-broken / rooted / malware infected device.
    ii Application must prevent hackers from accessing the application in a case where the device is rooted or jail broken.
    iii Blacklisting/Blocking of older versions of the Application on the back end, if there is a security breach.
r) Transaction Logs
    i Should maintain detailed transaction logs to enable processing audit trails to be reconstructed in the event of any disputes or errors
    ii The storage and retention period of logs should be parameterized
    iii Security safeguards should also be implemented to protect the information from unauthorized modification or destruction
    iv System should facilitate maintaining logs.
    v Provision to generate detailed reports, logs, audit trails

7.19.4 DR Setup - Activities are to be performed by Respective Solution OEM (supported by bidder)

1. Respective solution OEM along with the bidder has to ensure that DR setup is ready on the date of Go Live of respective Applications
2. Respective solution OEM along with the bidder should make necessary setup to enable the DR within the agreed timelines.
3. Respective solution OEM along with the bidder should carry out the deployment of the application in DC and DR, UAT as applicable.
4. To ensure proper rollback, Respective solution OEM along with the bidder has to ensure that the old setup at all the locations is as–IS as per the agreed timelines during migration strategy formulation.

8 CONTRACT PERIOD

The terms and conditions of purchase order and RFP (read with addendums/Corrigendum/ Clarifications) shall constitute a binding contract.

The Bidder is required to sign the contract within 15 days from the date of acceptance of the Purchase Order.

The contract period for the project is the Implementation Period (as mentioned in Section 9: Project Timelines) + Support period (60 Month Post Go-live) which will commence from the date of acceptance of PO. Effective start date for the contract would be date of acceptance of the PO.

The bank may, at its sole discretion, extend the contract for an additional period of two years, in one-year increments tranches. The Bank may extend the support services for an additional period of up to two (2) years beyond the original contract period. The pricing applicable during the extension period shall be mutually agreed and shall not exceed 120% of last year's AMC/ATS/Facility management rates quoted by the Selected Bidder.

The decision to further extend the contract with the same bidder shall be at the sole discretion of the Bank. Further, the Bank will have the right to renegotiate prices of AMC, ATS, Facility Management rates at the end of the contract period.

End of Sales / End of support:
The proposed IT Infrastructure/Hardware Appliances model should not be end of sale product at the time of bid submission, and supportability (End of Life or End of support) of the product should be available for the entire contract period.
Bidder to submit the undertaking on OEMs Letterhead (refer Undertaking: Support & Launch Confirmation
Bidder to submit the undertaking on IT Infrastructure OEM's letterhead as per Annexure 26: Undertaking – Support & Launch Confirmation.
In the event if any equipment supplied by the bidder reaches the end of support, within the contract period, the bidder has to replace the equipment/component at no additional cost to the Bank.
During the extension period, if any product goes end of support bidder is required to provide the extended OEM support for proposed product or provide the bank with the alternative product of similar/higher configuration from OEM (with requisite support) at no additional cost to the bank.

The Pre-Contract Integrity Pact Agreement submitted by the bidder during Bid submission will automatically form a part of the Contract Agreement till the conclusion of the contract, including extended period.

9 PROJECT TIMELINES

Overall Implementation period shall be 5 Months (Start Date is T0) for all solution & services.
The bidder shall submit a comprehensive Project Plan, within 7 days of T0 covering each proposed product/solution & Services, detailing all project phases, milestones, tasks, sub-tasks, activities, timelines, dependencies.

The bidder shall submit the detailed Project Plan along with the proposal (mandatory) and subsequently within seven (7) days from T0 for the Bank's review and approval.
Any Liquidated Damages (LD) for delays in project execution shall be calculated based on the bank's approved Project Plan.

In the event the bidder fails to submit the Project Plan within seven (7) days from T0, the Bank reserves the right to levy applicable Liquidated Damages for each day of such delay. If the delay in submission of project plan exceeds seven (7) days, the Bank may prepare and issue the Project Plan, which shall be final and binding on the bidder.

The bidder shall execute the project in accordance with the Bank-issued Project Plan, maintaining the overall implementation period of five (5) months from T0.
All applicable Service Level Agreements (SLAs), milestones, Liquidated Damages (LDs), and other contractual obligations shall thereafter be governed by the Bank-issued Project Plan, which shall be deemed to have been accepted by the bidder without any further objection or reservation.
All the requirement marked by bidder as “S” and “C” has to be delivered before UAT
T0- Date of acceptance of PO

10 EVALUATION CRITERIA

10.1 Preliminary Scrutiny

1. The Bank will examine the Bids to determine whether they are complete, required formats have been furnished, the documents have been properly signed, and the Bids are generally in order.
2. The Bank may, at its discretion, waive any minor infirmity, non-conformity, or irregularity in a Bid, which does not constitute a material deviation.
3. The Bank will determine the responsiveness of each Bid to the Bidding Document. For the purposes of these Clauses, a responsive Bid is one which conforms to all the terms and conditions of the Bidding Document without material deviations. Deviations from, or objections or reservations to critical provisions, such as those concerning Bid Security, Applicable Law, Bank Guarantee will be deemed to be a material deviation.
4. The Bank's determination of a Bid's responsiveness will be based on the contents of the Bid itself, without recourse to extrinsic evidence. The Bank reserves the right to evaluate the bids on technical and functional parameters, including possible visits to inspect live site/s of the Bidder and witness demos of the system and verify functionalities, response times, etc.
5. If a Bid is not responsive, it will be rejected by the Bank and may not subsequently be made responsive by the Bidder by correction of the non-conformity.
6. If any information / data / particulars are found to be incorrect, bank will have the right to disqualify the company, take appropriate action and invoke the performance bank guarantee/ EMD

A stage bid system is adopted for selection of the bidder:

- Stage 1 – Eligibility and Technical Bid evaluation
- Stage 2 – Commercial Bid Evaluation

During evaluation of the Tenders, the Bank, at its discretion, may ask the Bidder for clarification in respect of its tender. The request for clarification and the response shall be in writing, and no change in the substance of the tender shall be sought, offered, or permitted. The Bank reserves the right to accept or reject any tender in whole or in part without assigning any reason thereof. The decision of the Bank shall be final and binding on all the bidders to this document and the bank will not entertain any correspondence in this regard.

The evaluation of bids shall be based on the documents, credentials, experience references, and information submitted by the bidder as part of its bid response on or before the bid submission deadline. Any new credential, experience reference, document, or supporting evidence that was not originally submitted with the bid may, at the Bank's discretion, not be accepted or considered during the evaluation process. Bidders are therefore advised to ensure that all required documents and supporting evidence are submitted along with the bid. The Bank shall evaluate the bid based on the documents submitted

and the Bank's decision regarding the adequacy, relevance, interpretation, compliance, and evaluation of the submitted documents and information shall be final, conclusive, and binding on all bidders.
=-.

10.2 Eligibility Evaluation Criteria

#	Eligibility Criteria/Clause	Documents Required
1.	Proof of Earnest Money Deposit	To be submitted along with the bid.
2.	The Bidder should be operating in India as a registered company under Companies Act, 2013/1956 or LLP (Limited Liability Partnership) Act 2008 or Partnership firms registered under the Indian Partnership Act, 1932 with registered offices in India, and should be in existence in India for at least the last 5 (five) years as on date of opening of the bid	Copy of Certificate of Incorporation or Partnership Deed AND Copy of Registration Certificate/GST Registration certificate Copies of all documents listed above should be attested by authorized signatory and must be submitted along with the response.
3.	The bidder should have valid PAN and GST Registration in India	Copy of Valid PAN Card, GST Registration Certificates issued by competent authority in India
4.	The bidder should have a minimum average turnover of INR 500 crore per annum in India during the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth. Note – In case of MSMEs only, the turnover may be relaxed subject to meeting the quality and technical specifications.	CA Certificate mentioning the turnover and net worth for each financial year. and Audited Financial statements (Balance sheet & Profit & Loss statement). The CA certificate provided in this regard should be without any riders or qualification.
5.	The bidder should be an authorized representative/ partner/ reseller of OEM in India. MAF should be submitted from the following solution OEMs: 1. SIEM 2. SOAR 3. UEBA	MAF from the respective OEMs of the solution & services containing- 1. Name and address of the OEM and the name and address of the authorised bidder/entity. 2. Confirmation that the bidder/entity is duly authorised by the OEM for supply, installation, implementation, technical support, maintenance and related services for the proposed solution(s).

#	Eligibility Criteria/Clause	Documents Required
	4. Extended Detection & response (XDR) 5. Decoy/HoneyPot/Deception 6. Threat Intelligence Platform 7. Vulnerability Assessment & vulnerability Lifecycle Management 8. Identity Threat Detection & response 9. Application Security Testing 10. Cloud Security Posture Management (CSPM) 11. Cloud-Native Application Protection Platform (CNAPP) 12. Cloud Workload Protection Platform (CWPP) 13. Continuous Threat Exposure Management (CTEM) MAF should also be submitted from the following services OEMs: 1. Breach Attack & Simulation 2. Continuous Automated Red Teaming services 3. Attack Surface management 4. Phishing simulation 5. Digital Risk Management 6. Dark web monitoring 7. Threat Intelligence feed 8. Threat hunting services	The MAF shall be submitted on the official letterhead of the respective OEM and must be signed by an authorised signatory having the authority to bind the OEM."
6.	Bidder must have at least enrolled manpower (on bidder's payroll) of 100 experienced employees skilled in areas of Cyber security.	Self-certification from the bidder
7.	The bidder must have experience of having successfully installed and maintained (and currently maintaining) and/or managing the SIEM Solution, with a minimum capacity of 20,000 EPS / 0.86 TB per day, as stipulated in the RFP, for a	Bidder to Submit the following 3 Documents: Document 1: Copy of Purchase Order / Work Order / Contract

#	Eligibility Criteria/Clause	Documents Required
	single eligible client falling within the categories specified in the RFP, in India, during the last five years. The stipulated 20,000 EPS / 0.86 TB per day requirement shall be demonstrated for a single eligible client and a single SIEM deployment/environment. Note: - experience shall be considered irrespective of when the implementation was completed. Even if the implementation was completed more than five years prior to the date of publication of the RFP, such experience shall qualify only where the same Bidder that supplied, installed and implemented the SIEM Solution is also currently maintaining the same solution, or has maintained the same solution at any time during the five-year period preceding the date of publication of the RFP. The aggregate EPS/log volume of multiple tenants, clients, subsidiaries, sites, SIEM instances or separate deployments shall not be considered for meeting the stipulated threshold.	The submitted client-issued document shall clearly indicate, either directly or through a combination of documents forming part of the same contract: a. Name of the Client. b. Date of Issue/Signing. c. Scope of Work demonstrating - installation and maintenance/AMC/support of the SIEM Solution. d. Solution Name and OEM Name e. SIEM Sizing/Capacity implemented, clearly indicating minimum 20,000 EPS or 0.86 TB/day AND Document 2: Client-Issued Supporting Document (Any-One) Any one of the following client-issued documents: a. Client Credential/Experience Certificate; or b. Email Confirmation from the Client clearly stating the PO Number.; or c. Client-signed Installation/Implementation Report; or d. Client Acceptance/Go-Live/Completion/Sign-off Certificate; or e. Extension Letter The client-issued supporting document shall clearly establish, as applicable: • Name of the Client. • Project/Solution Name.

#	Eligibility Criteria/Clause	Documents Required
		• Successful - Installation and Commissioning/Implementation of the SIEM Solution. • Maintenance/Support/AMC status (completed or under maintenance). • SIEM Capacity implemented (EPS and/or TB/day) • Date(s) establishing that the project falls within the required eligibility period. AND Document 3: Bidder's Self-Declaration (in the format Annexure 22A) The Bidder shall submit a Self-Declaration cross-referencing the submitted documentary evidence and providing the following details: a. Project Name. b. Client Name. c. Client Category (PSU/ PSE/ Government Organizations / BFSI/Telecom). d. Scope Executed: e. - f. Installation – Yes/No g. Maintenance / Under Maintenance – Yes/No h. Contract Period: 1. Start Date 2. End Date i. Solution Name. j. OEM Name. k. Implemented SIEM Capacity (EPS and/or TB/day).

#	Eligibility Criteria/Clause	Documents Required
		l. Reference to the submitted client-issued document(s), including: 1. Document Name. 2. Relevant Page Number(s). 3. Clause/Section/Page where the following are evidenced: i. Client Name. ii. Scope of Work. iii. Solution Name. iv. SIEM Capacity (EPS/TB/day). v. Maintenance/Support Status. vi. Contract/Project Period.
8.	Bidder should have supplied, installed and maintained (or under maintenance) any three (3) of the below solutions in any one PSU/PSE/ Government Organizations / BFSI/Telecom provider in India a. SOAR b. UEBA c. Extended Detection & response (XDR)/ Endpoint Detection & response (EDR) d. Threat Intelligence Platform e. Vulnerability Assessment/Vulnerability management f. Identity Threat Detection & response g. Decoy/Honeypot/Deception h. Application security testing tool (DAST or SAST) i. Cloud Security Posture Management (CSPM) j. Cloud-Native Application Protection Platform (CNAPP) k. Cloud Workload Protection Platform (CWPP) l. Continuous Threat Exposure Management (CTEM)	Bidder to Submit the following 3 Documents: Document 1: Copy of Purchase Order / Work Order / Contract The submitted client-issued document shall clearly indicate, either directly or through a combination of documents forming part of the same contract: a. Name of the Client. b. Date of Issue/Signing. c. Scope of Work demonstrating supply, installation and maintenance/AMC/support of the respective Solution. d. Solution Name and OEM Name AND Document 2: Client-Issued Supporting Document (Any-One) Any one of the following client-issued documents: a. Client Credential/Experience Certificate;

#	Eligibility Criteria/Clause	Documents Required
	Note: - Experience of solutions can be shown in single /multiple Clients/ work orders meeting the above criteria - experience in - installing a solution will be considered regardless of when the installation was completed. Even if the installation was completed more than five years ago, it will still qualify, provided that the same bidder is currently maintaining that solution or has carried out its maintenance at any time during the five-year period preceding the RFP publication date	or b. Email Confirmation from the Client; or c. Client-signed Installation/Implementation Report; or d. Client Acceptance/Go-Live/Completion/Sign-off Certificate; or e. Extension Letter The client-issued supporting document shall clearly establish, as applicable: • Name of the Client. • Project/Solution Name. • Successful - Installation and Commissioning/Implementation. • Maintenance/Support/AMC status (completed or under maintenance). • Date(s) establishing that the project falls within the required eligibility period. Note: If all the above information is not available in a single client-issued document, the Bidder may submit a combination of client-issued documents, provided that together they establish compliance with the eligibility criteria. AND Document 3: Bidder's Self-Declaration (in the format Annexure 22A) The Bidder shall submit a Self-Declaration cross-referencing the submitted documentary evidence and providing the following details:

#	Eligibility Criteria/Clause	Documents Required
		a. Project Name. b. Client Name. c. Client Category (PSU/PSE/ Government Organizations / BFSI/Telecom) d. Scope Executed: e. - f. Installation – Yes/No g. Maintenance / Under Maintenance – Yes/No h. Contract Period: a. Start Date b. End Date i. Solution Name. j. OEM Name. k. Reference to the submitted client-issued document(s), including: a. Document Name. b. Relevant Page Number(s). c. Clause/Section/Page where the following are evidenced: i. Client Name. ii. Scope of Work. iii. Solution Name. iv. Maintenance/Support Status. v. Contract/Project Period.
9.	Bidder must have back-to-back support relation with the proposed OEMs of solutions & services.	Self-Declaration from the bidder's authorized signatory as per the format Annexure 33: Confirmation for Backlining
10.	If the bidder or its subsidiary or its associate or sister company or its holding company has already had an association with Punjab & Sind Bank in the past 5 years or at present as a service provider on any project, then the bidder is required to	Self-Certification from the bidder in the format Annexure 27: Association with Bank

#	Eligibility Criteria/Clause	Documents Required
	submit the satisfactory certificate from the bank issued/dated post the issuance of the RFP. Additionally, the Bidder should not have any Service Level Agreement/Contract pending to be signed with the Bank pending for more than 6 months from the date of issue of purchase order	
11.	The Bidder to provide information that none of its subsidiaries or sister company or associate or holding company or companies having common director/s or companies in the same group of promoters/management or partnership firms/LLPs having common partners is not owned by any Director or Employee of the Bank.	Self-Certification from the bidder (in the format Annexure 28: Ownership Declaration and Contractual performance)
12.	The bidder shall submit a self-declaration confirming that, during the last three (3) years preceding the date of publication of this RFP, no contract, Purchase Order, or award issued by Punjab & Sind Bank (PSB) to the bidder has been cancelled, terminated, rescinded, or revoked due to non-performance, breach of obligations, or failure to comply with post-award requirements.	Self-Certification from the bidder (in the format Annexure 29: Contract Cancellation / Termination / Rescission / Revocation)
13.	The Bidder should not have been blacklisted/ debarred by the Regulator / statutory body/ Government / Government agency / Banks / Financial Institutions in India during last 3 years and as on the date of bid submission.	Self-Certification from the bidder as per Annexure 11
14.	The bidder should not be involved in any litigation which threatens the solvency of company.	Self-Certification from the bidder as per Annexure 10
15.	Labor Law Compliance	Self-Certification from the bidder as per the format provided in Annexure 30

#	Eligibility Criteria/Clause	Documents Required
16.	Integrity Pact	Document on 100 Rs Stamp paper, duly signed and stamped by the authorized signatory. (As per Annexure 17)
17.	Non-Disclosure Agreement	Document on 100 Rs Stamp paper, duly signed and stamped by the authorized signatory. (As per Annexure 13)
18.	To ensure conflict of interest the successful bidder or its subsidiary or its associate or sister company or its holding company should not be **the IT Security or NOC vendor** of the bank under the existing or new contract	Self-declaration signed by Authorized Signatory of the bidder (as per Annexure 31)
OEM Evaluation Criteria		
19.	The proposed OEM SIEM Solution with a minimum capacity of 30,000 EPS or 1.2 TB/day shall have been successfully implemented and be under management/maintenance in at least one (1) BFSI client in India. The stated minimum capacity of 30,000 EPS or 1.2 TB/day shall be demonstrated in the referenced client only and shall not be aggregated or combined across multiple clients/references. **and** The proposed OEM SIEM Solution with a minimum capacity of 30,000 EPS or 1.2 TB/day shall have been successfully implemented on cloud in atleast one (1) client in India. The stated minimum capacity of 30,000 EPS or 1.2 TB/day shall be demonstrated in the referenced client only and shall not be aggregated or combined across multiple clients/references. Note: -	Document 1: Copy of Purchase Order / Work Order / Contract The submitted client-issued document shall clearly indicate, either directly or through a combination of documents forming part of the same contract: a. Name of the Client. b. Date of Issue/Signing. c. Scope of Work. d. Solution Name and OEM Name e. SIEM Capacity, clearly indicating one of the following, as applicable: a. Minimum 30,000 EPS or 1.2 TB/day. b. On-premises/Cloud Deployment OR Document 2: Client-Issued Supporting Document (Any-One) Any one of the following client-issued documents: a. Client Credential/Experience Certificate; or b. Email Confirmation from the Client;

#	Eligibility Criteria/Clause	Documents Required
	experience in - installing a solution will be considered regardless of when the installation is completed. Even if the installation was completed more than five years ago, it will still qualify, provided that the same bidder is currently maintaining that solution or has carried out its maintenance at any time during the five-year period preceding the RFP publication date. The aggregate EPS/log volume of multiple tenants, clients, subsidiaries, sites, SIEM instances or separate deployments shall not be considered for meeting the stipulated threshold.	or c. Client-signed Installation/Implementation Report; or d. Client Acceptance/Go-Live/Completion/Sign-off Certificate; or e. AMC/Support Confirmation/Extension Letter or f. Client-issued Project Status/Progress Certificate (for projects under implementation) The client-issued supporting document shall clearly establish, as applicable: • Name of the Client. • Project/Solution Name. • Project Status, clearly indicating one of the following o Implemented & Managed; o Under Maintenance/Managed Services; o Under Implementation. • SIEM Capacity implemented/under implementation (EPS and/or TB/day) • Date(s) establishing that the project falls within the required eligibility period. Note: If all the above information is not available in a single client-issued document, the Bidder may submit a combination of client-issued documents, provided that together they establish compliance with the eligibility criteria. AND

#	Eligibility Criteria/Clause	Documents Required
		Document 3: OEM's Self-Declaration (as per **Annexure 22B: OEM Self-Declaration for Implementation Experience)** The OEM shall submit a Self-Declaration cross-referencing the submitted documentary evidence and providing the following details: a. Project Name. b. Client Name. c. Client Category (BFSI). d. Contract Period: a. Start Date b. End Date e. Solution Name. f. Project Status (Select one): a. Implemented & Managed; b. Under Maintenance; c. Under Implementation. g. SIEM Capacity (EPS and/or TB/day). h. Reference to the submitted client-issued document(s), including: a. Document Name. b. Relevant Page Number(s). c. Clause/Section/Page where the following are evidenced: i Client Name. ii Scope of Work. iii Solution Name. iv SIEM Capacity (EPS/TB/day). v Maintenance/Support Status. vi Contract/Project Period.

#	Eligibility Criteria/Clause	Documents Required
		vii Project Status (Implemented & Managed / Under Maintenance / Under Implementation)
20.	The proposed OEM solution should have been implemented in at least one BFSI client is to be submitted for the following solutions: 1. SOAR 2. UEBA 3. Extended Detection & response (XDR) 4. Threat Intelligence Platform Note: - Experience of solutions can be shown in single /multiple Clients/ work orders meeting the above criteria A bidder's experience in - installing a solution will be considered regardless of when the installation was completed. Even if the installation was completed more than five years ago, it will still qualify, provided that the same bidder is currently maintaining that solution or has carried out its maintenance at any time during the five-year period preceding the RFP publication date	Document 1: Copy of Purchase Order / Work Order / Contract The submitted client-issued document shall clearly indicate, either directly or through a combination of documents forming part of the same contract: a. Name of the Client. b. Date of Issue/Signing. c. Scope of Work demonstrating - installation and maintenance/AMC/support of the respective Solution. d. Solution Name and OEM Name OR Document 2: Client-Issued Supporting Document (Any-One) Any one of the following client-issued documents: a. Client Credential/Experience Certificate; or b. Email Confirmation from the Client; or c. Client-signed Installation/Implementation Report; or d. Client Acceptance/Go-Live/Completion/Sign-off Certificate; or e. AMC/Support Confirmation/Extension Letter The client-issued supporting document shall clearly establish, as applicable: • Name of the Client.

#	Eligibility Criteria/Clause	Documents Required
		• Project/Solution Name. • Successful - Installation and Commissioning/Implementation. • Maintenance/Support/AMC status (completed or under maintenance). • Date(s) establishing that the project falls within the required eligibility period. Note: If all the above information is not available in a single client-issued document, the Bidder may submit a combination of client-issued documents, provided that together they establish compliance with the eligibility criteria. AND Document 3: OEM's Self-Declaration (as per **Annexure 22B: OEM Self-Declaration For Implementation Experience)** The OEM shall submit a Self-Declaration cross-referencing the submitted documentary evidence and providing the following details: 1. Project Name. 2. Client Name. 3. Client Category (BFSI) 4. Scope Executed: 5. - 6. Installation – Yes/No 7. Maintenance / Under Maintenance – Yes/No 8. Contract Period: a. Start Date b. End Date 9. Solution Name.

#	Eligibility Criteria/Clause	Documents Required
		10. OEM Name. 11. Reference to the submitted client-issued document(s), including: a. Document Name. b. Relevant Page Number(s). c. Clause/Section/Page where the following are evidenced: i. Client Name. ii. Scope of Work. iii. Solution Name. iv. Maintenance/Support Status. v. Contract/Project Period.
21.	The proposed OEM solution should have been implemented in at least one Scheduled Commercial Bank/PSU/ PSE/Government Organizations / BFSI/ in India. Credential is to be submitted for the following solutions: 1. Decoy/Honey-Pot/Deception 2. Vulnerability Assessment/Vulnerability management 3. Identity threat detection and response (ITDR) 4. Application Security testing Tool (SAST & DAST) 5. Cloud Security solution (CSPM) Note: - Experience of solutions can be shown in single /multiple Clients/ work orders meeting the above criteria A bidder's experience in - installing a solution will be considered regardless of when the installation was completed. Even if the installation was completed more than five years ago, it will still qualify, provided the bidder is currently	Document 1: Copy of Purchase Order / Work Order / Contract The submitted client-issued document shall clearly indicate, either directly or through a combination of documents forming part of the same contract: a. Name of the Client. b. Date of Issue/Signing. c. Scope of Work demonstrating , installation and maintenance/AMC/support of the respective Solution. d. Solution Name and OEM Name OR Document 2: Client-Issued Supporting Document (Any-One) Any one of the following client-issued documents: a. Client Credential/Experience Certificate; or b. Email Confirmation from the Client; or

#	Eligibility Criteria/Clause	Documents Required
	maintaining that solution or has carried out its maintenance at any time during the five-year period preceding the RFP publication date	c. Client-signed Installation/Implementation Report; or d. Client Acceptance/Go-Live/Completion/Sign-off Certificate; or e. AMC/Support Confirmation/Extension Letter The client-issued supporting document shall clearly establish, as applicable: • Name of the Client. • Project/Solution Name. • Successful - Installation and Commissioning/Implementation. • Maintenance/Support/AMC status (completed or under maintenance). • Date(s) establishing that the project falls within the required eligibility period. Note: If all the above information is not available in a single client-issued document, the Bidder may submit a combination of client-issued documents, provided that together they establish compliance with the eligibility criteria. AND Document 3: OEM's Self-Declaration (as per **Annexure 22B: OEM Self-Declaration For Implementation Experience)** The OEM shall submit a Self-Declaration cross-referencing the submitted documentary evidence and providing the following details: 1. Project Name.

#	Eligibility Criteria/Clause	Documents Required
		2. Client Name. 3. Client Category (Scheduled Commercial Bank/PSU/ PSE/Government Organizations / BFSI/) 4. Scope Executed: 5. - 6. Installation – Yes/No 7. Maintenance / Under Maintenance – Yes/No 8. Contract Period: c. Start Date d. End Date 9. Solution Name. 10. OEM Name. 11. Reference to the submitted client-issued document(s), including: a. Document Name. b. Relevant Page Number(s). c. Clause/Section/Page where the following are evidenced: i. Client Name. ii. Scope of Work. iii. Solution Name. iv. Maintenance/Support Status. v. Contract/Project Period.
22.	The proposed OEM solution should have been implemented in at least one verifiable client in India. Credential is to be submitted for the following solutions: a. CNAPP b. CWPP	Document 1: Copy of Purchase Order / Work Order / Contract The submitted client-issued document shall clearly indicate, either directly or through a combination of documents forming part of the same contract: a. Name of the Client. b. Date of Issue/Signing.

#	Eligibility Criteria/Clause	Documents Required
	c. CTEM Note: - Experience of solutions can be shown in single /multiple Clients/ work orders meeting the above criteria experience in - installing a solution will be considered regardless of when the installation was completed. Even if the installation was completed more than five years ago, it will still qualify, provided the bidder is currently maintaining that solution or has carried out its maintenance at any time during the five-year period preceding the RFP publication date	c. Scope of Work demonstrating installation and maintenance/AMC/support of the respective Solution. d. Solution Name and OEM Name OR Document 2: Client-Issued Supporting Document (Any-One) Any one of the following client-issued documents: a. Client Credential/Experience Certificate; or b. Email Confirmation from the Client; or c. Client-signed Installation/Implementation Report; or d. Client Acceptance/Go-Live/Completion/Sign-off Certificate; or e. AMC/Support Confirmation/Extension Letter The client-issued supporting document shall clearly establish, as applicable: • Name of the Client. • Project/Solution Name. • Successful Installation and Commissioning/Implementation. • Maintenance/Support/AMC status (completed or under maintenance). • Date(s) establishing that the project falls within the required eligibility period. Note: If all the above information is not available in a single client-issued document, the Bidder may submit a combination of client-

#	Eligibility Criteria/Clause	Documents Required
		issued documents, provided that together they establish compliance with the eligibility criteria. AND Document 3: OEM's Self-Declaration (as per **Annexure 22B: OEM Self-Declaration For Implementation Experience)** The OEM shall submit a Self-Declaration cross-referencing the submitted documentary evidence and providing the following details: a. Project Name. b. Client Name. c. Client Category (Scheduled Commercial Bank/PSU/ PSE/Government Organizations / BFSI/ Fortune 500 Companies (2024/2025/2026) d. Scope Executed: e. - f. Installation – Yes/No g. Maintenance / Under Maintenance – Yes/No h. Contract Period: a. Start Date b. End Date i. Solution Name. j. OEM Name. k. Reference to the submitted client-issued document(s), including: a. Document Name. b. Relevant Page Number(s).

#	Eligibility Criteria/Clause	Documents Required
		c. Clause/Section/Page where the following are evidenced: i. Client Name. ii. Scope of Work. iii. Solution Name. iv. Maintenance/Support Status. v. Contract/Project Period.
23.	The proposed OEM services should have been implemented in at least one (1) PSU/ PSE/ Government Organizations / BFSI in India. Credential is to be submitted for the following services: 1. Breach Attack & Simulation 2. Continuous Automated Red Teaming 3. Attack surface management 4. Phishing simulation 5. Dark web monitoring 6. Threat Intelligence feed 7. Threat Hunting services 8. Either Digital Risk Management Services, OR both Anti-Phishing and Brand Protection & Monitoring Services.	Document 1: Copy of Purchase Order / Work Order / Contract The submitted client-issued document shall clearly indicate, either directly or through a combination of documents forming part of the same contract: a. Name of the Client. b. Date of Issue/Signing. c. Scope of Work demonstrating , installation and maintenance/AMC/support of the respective service. d. Solution Name and OEM Name OR Document 2: Client-Issued Supporting Document (Any-One) Any one of the following client-issued documents: a. Client Credential/Experience Certificate; or b. Email Confirmation from the Client; or c. Client-signed Installation/Implementation Report; or d. Client Acceptance/Go-Live/Completion/Sign-off Certificate; or

#	Eligibility Criteria/Clause	Documents Required
		e. AMC/Support Confirmation/Extension Letter The client-issued supporting document shall clearly establish, as applicable: • Name of the Client. • Project/service Name. • Successful Installation and Commissioning/Implementation. • Maintenance/Support/AMC status. • Date(s) establishing that the project falls within the required eligibility period. Note: If all the above information is not available in a single client-issued document, the Bidder may submit a combination of client-issued documents, provided that together they establish compliance with the eligibility criteria. AND Document 3: OEM's Self-Declaration (as per **Annexure 22B: OEM Self-Declaration For Implementation Experience)** The OEM shall submit a Self-Declaration cross-referencing the submitted documentary evidence and providing the following details: a. Project Name. b. Client Name. c. Client Category (PSU / PSE / Government Organization / BFSI) d. Scope Executed: a. - b. Installation – Yes/No

#	Eligibility Criteria/Clause	Documents Required
		c. Maintenance / Under Maintenance – Yes/No e. Contract Period: a. Start Date b. End Date f. Service Name. g. OEM Name. h. Reference to the submitted client-issued document(s), including: a. Document Name. b. Relevant Page Number(s). c. Clause/Section/Page where the following are evidenced: i. Client Name. ii. Scope of Work. iii. Solution Name. iv. Maintenance/Support Status. v. Contract/Project Period.
24.	Compliance Confirmation from respective solution and services OEM Solution List: 1. SIEM 2. SOAR 3. UEBA 4. Extended Detection & response (XDR) 5. Decoy/Honey-Pot/Deception 6. Threat Intelligence Platform 7. Vulnerability assessment (VA) & vulnerability lifecycle management 8. Identity threat detection and response	Declaration in the format as mentioned in Annexure 18. FRS and TRS compliance sheet (Excel) are to be submitted along with the self-declaration.

#	Eligibility Criteria/Clause	Documents Required
	9. Application Security testing Tool (SAST & DAST) 10. Cloud Security solution (CSPM) 11. CNAPP 12. CWPP 13. CTEM Services List: 1. Breach Attack & Simulation 2. Continuous Automated Red Teaming 3. Attack Surface management 4. Phishing simulation 5. Digital Risk Management 6. Dark web monitoring 7. Threat Intelligence feed 8. Threat hunting services	
25.	Functional Compliance: The Bidder's proposed solution shall be evaluated for functional compliance against the requirements specified in Appendix 1A: Functional Compliance Sheet. The proposed product should have minimum functional compliance score of 85% for each of the following: Solution List: 1. SIEM 2. SOAR 3. UEBA 4. Extended Detection & response (XDR)	a) OEM Self Declaration (Annexure 32) b) Filled Appendix 1A & 1C: Functional Compliance Supporting Documentation like datasheets, product manuals, OEM website product feature listings etc. The Declaration is to be submitted by the OEMs of the following solution and services

#	Eligibility Criteria/Clause	Documents Required
	5. Decoy/Honey-Pot/Deception 6. Threat Intelligence Platform 7. Vulnerability assessment (VA) & vulnerability lifecycle management 8. Identity threat detection and response 9. Application Security testing Tool (SAST & DAST) 10. Cloud Security solution (CSPM) 11. CNAPP 12. CWPP 13. CTEM Services List: 1. Breach Attack & Simulation 2. Continuous Automated Red Teaming 3. Attack Surface management 4. Phishing simulation 5. Digital risk management 6. Dark web monitoring 7. Threat Intelligence feed 8. Threat hunting services Each product/solution shall be evaluated independently, and the compliance score shall be computed separately for each product/solution. Maximum Marks | Compliance (S/C) | Maximum Mark	

#	Eligibility Criteria/Clause			Documents Required
	10	S (Standard):	This indicates that the requirement is covered by the standard product functionality. It includes features available out-of-the-box, as well as those achievable through parametrization or rules configuration.	
	3	C (Customization):	Requirements marked as "C" are the ones that require minor modifications to the proposed solution. 1. Such customizations may include development of custom code, creation of new interfaces, user interface enhancements, or custom-built screens integrated with the base product. 2. All identified customizations shall be completed, tested, and made available by the bidder prior to commencement of User Acceptance Testing	

#	Eligibility Criteria/Clause	Documents Required
	(UAT), without impacting the Bank's project timelines. 3. Only those changes that can be implemented without altering the base product and without impacting future upgrades, patches, or vendor support shall qualify as Customization (C)	

Note: In the event a Bidder participates in both the NextGen SOC RFP and IT Security solution & services RFP (GEM/2026/B/7936763 and GEM/2026/B/7752177) and is declared the successful bidder in either of the RFPs after completion of the commercial evaluation process, such Bidder shall be deemed ineligible for award in the other RFP. Accordingly, the commercial bid of such Bidder for the other RFP shall not be opened or, if already opened, shall not be considered for evaluation or award by the Bank. The decision of the Bank in this regard shall be final and binding.

a. Attested copies of all relevant documents, certificates, work orders, completion certificates, financial statements, and other supporting documents shall be submitted as documentary evidence in support of the claims made by the bidder. The bidder shall furnish any additional information and clarification as may be required by the Bank for verification of eligibility criteria. The Bank reserves the right to independently verify, evaluate, and validate the information and claims submitted by the bidder. The decision of the Bank in this regard shall be final, conclusive, and binding on the bidder.
b. In the event of a business transfer, acquisition, slump sale, merger, or acquisition of a business undertaking, the work experience, credentials, and references of the transferor entity ("Seller") pertaining to the acquired business may be considered, subject to submission of documentary evidence establishing such transfer and continuity of business operations.

c. In cases involving corporate restructuring, including merger, amalgamation, demerger, name change, conversion, or reorganization, the incorporation certificate, financial statements, work experience credentials, technical qualifications, and other relevant records of the predecessor entity may be considered, subject to submission of documentary evidence acceptable to the Bank.
d. Either the Principal/OEM or its authorized agent may submit a bid for a given item/product under this RFP. However, both the Principal/OEM and its authorized agent shall not be permitted to submit bids simultaneously for the same item/product in the same RFP. Further, where an agent is authorized to represent a Principal/OEM, the same agent shall not submit bids on behalf of more than one Principal/OEM for the same item/product under this RFP. Any violation of the above conditions shall render all such bids liable for rejection at the sole discretion of the Bank.
e. The bidder and/or OEM shall comply with applicable guidelines issued by the Central Vigilance Commission (CVC), including Circular No. 03/01/12, the applicable provisions of the General Financial Rules (GFR), and the Department of Expenditure Office Memorandum dated 25.07.2016, as amended from time to time.
f. In a tender, either the Indian Agent on behalf of the Principal/OEM or the Principal/OEM itself may bid; however, both shall not bid simultaneously for the same item/product in the same tender.
g. Documentary evidence shall be furnished against each eligibility criterion along with a detailed index of documents submitted. All documents shall be duly signed and stamped by the Authorized Signatory of the bidder. Relevant sections of the submitted documents supporting compliance with the eligibility criteria shall be clearly highlighted for ease of verification by the Bank.
h. Any misrepresentation, suppression of facts, submission of forged/fabricated documents, or provision of incorrect information by the bidder at any stage of the bidding process may result in rejection of the bid, forfeiture of bid security (if applicable), and/or blacklisting/debarment from participating in future procurement processes of the Bank, without prejudice to any other rights and remedies available to the Bank under law.
i. For the purpose of this RFP, the term "Scheduled Bank" shall exclude Regional Rural Banks (RRBs) and Payment banks. Accordingly, experience shall be considered for the purpose of evaluating eligibility and qualification criteria under this RFP.
j. Deployments shall be considered valid only if the solution has been used for its intended function in a production environment. Tests, pilot, or non-production deployments shall not be accepted.
k. Experience of solution(s) can be shown in single /multiple Clients/work orders meeting the criteria(s)
l. Experience should be during the five-year period preceding the RFP publication date. Even if the installation was completed more than five years ago, it will still qualify, provided the product is currently under maintenance or has been maintained at any time during the five-year period preceding the RFP publication date
m. Experience must be showcased separately for each solution category, with clear evidence that each solution has been deployed as a standalone solution and not merely as a feature or component of another solution.

n. When deemed necessary the Evaluation Committee may seek clarification on relevant aspects from the Bidder. However, that would not entitle the Bidder to change or cause any change.
o. Bank reserves the right to conduct reference site visit/ video conference/ voice call with the Client to substantiate the credentials/ copy of PO/ Contract copy/ sign-off submitted by Bidder and/ or OEM. In case the input/ feedback received from the Customer is negative/ unsatisfactory, bank reserves the right to reject the Bid.

10.3 Technical Evaluation Criteria

Only those bidders who are found to be responsive and who meet all the Pre-Qualification (PQ) (Section 10.2) Criteria of the RFP, as determined by the Bank, shall be evaluation for technical Evaluation Criteria (Section 10.3). Bidder must score minimum 80% overall technical score (80/100 marks). Marks obtained by the bidder under each line item of table will be normalized to their weightages as shown in the table summing to a total of 100

Commercial Price Bids will only be opened for bidders who qualify the minimum technical qualification criteria as detailed below

Note: The documents requirement remains same for the technical evaluation, refer the Section10.2 Eligibility Evaluation Criteria.

S.No.	Criteria	Scoring
Bidder's Scoring Criteria		
1	Bidder should have supplied, installed and maintained (or under maintenance) the below solutions in any one PSU/PSE/ Government Organizations / BFSI/Telecom provider in India 1. SOAR 2. UEBA 3. Extended Detection & response (XDR)/ Endpoint Detection & response (EDR)/Network detection & response (NDR/Network behavior anomaly detection (NBAD) 4. Threat Intelligence Platform 5. Vulnerability Assessment / Vulnerability Management 6. Identity Threat Detection & response (ITDR) 7. Decoy/Honeypot/Deception 8. Application security testing tool (DAST/SAST) 9. CSPM	Point 1: Experience in 3 solutions – 8 Marks Point 2: Experience in 4 solutions –10 Marks Point 3: Experience in 5 solutions –12 Marks Point 4: Experience in more than 5 solutions– 14 Marks Max Marks – 14 Marks
2	The Bidder must have successfully installed and maintained (and currently maintaining) and/or managing the SIEM Solution in at least	Point 1- 7 Marks Point 2- 10 Marks

S.No.	Criteria	Scoring
	one PSU/PSE, Government Organisation, BFSI organisation, Telecom provider, with demonstrated deployment experience meeting the following: 1. Point 1: 20000 EPS / 0.86 TB per day ≤ SIEM Solution Experience < 25,000 EPS / 1.00 TB per day 2. Point 2: 25,000 EPS / 1.00 TB per day ≤ SIEM Solution Experience < 30,000 EPS / 1.20 TB per day 3. Point 3: 30,000 EPS / 1.20 TB per day ≤ SIEM Solution Experience Note: The aggregate EPS/log volume of multiple tenants, clients, subsidiaries, sites, SIEM instances or separate deployments shall not be considered for meeting the stipulated threshold.	Point 3 – 15 Marks Max Marks – 15 Marks
OEM Evaluation Criteria		
3	The proposed OEM SIEM solution should have been implemented (and should be maintained/under-maintenance) in PSU/PSE, Government Organisation, BFSI organisation/Telecom/Fortune 500 (Last 3 years) in India with the following requirement as mentioned in the below category. Category: i. Category 1: 30000 EPS/ 1.2TB per day or more – 3 Marks ii. Category 2: 50000 EPS/ 2TB per day or more – 5 Marks iii. Category 3: 75000 EPS/ 3TB per day or more -- 7 Marks A maximum of two (2) credentials shall be considered for evaluation.	Max Marks – 15 Marks

S.No.	Criteria	Scoring
	For each qualifying credential pertaining to a Scheduled Commercial Bank (SCB), an additional 0.5 marks shall be awarded Even if the installation was completed more than five years ago, it will still qualify, provided the bidder is currently maintaining that solution or has carried out its maintenance at any time during the five-year period preceding the RFP publication date Note: The aggregate EPS/log volume of multiple tenants, clients, subsidiaries, sites, SIEM instances or separate deployments shall not be considered for meeting the stipulated threshold.	
4	The proposed OEM solution (solution list in mentioned below) should have been implemented in Client (BFSI/PSU/PSE/ Govt Organization) in India. Bidder to substantiate the clause for each of the below-mentioned solution and scoring for each of the solution would be summed to arrive at the solution OEM experience score. List of Solutions are: 1. SOAR 2. UEBA 3. Extended detection & response (XDR) 4. Decoy/HoneyPot/Deception 5. Threat Intelligence Platform 6. Vulnerability Assessment/Vulnerability Management 7. Identity Theft Detection & response 8. Application Security testing Tool (Both DAST & SAST) 9. Cloud Security posture Management tool (CSPM) Category:	Point 1 = 2 Marks Point 2 = 3 Marks Max Marks – 27 Marks

S.No.	Criteria	Scoring
	a. Point 1: = 1 Client b. Point 2: ≥ 2 Client Even if the installation was completed more than five years ago, it will still qualify, provided the bidder is currently maintaining that solution or has carried out its maintenance at any time during the five-year period preceding the RFP publication date	
5	The proposed OEM solution should have been implemented in verifiable client in India. Credential is to be submitted for each of the following solutions: 1. CNAPP 2. CWPP 3. CTEM Category: a. Point 1: = 1 Client b. Point 2: ≥ 2 Client Even if the installation was completed more than five years ago, it will still qualify, provided the bidder is currently maintaining that solution or has carried out its maintenance at any time during the five-year period preceding the RFP publication date	Point 1 = 1 Mark Point 2 = 2 Marks Max Marks – 6 Marks
6	The proposed OEM services (below mentioned to the services) should have been implemented in Client (BFSI/PSU/PSE/ Govt Organization) in India. Bidder to substantiate the clause for each of the below mentioned OEM service and scoring for each of the service would be summed to arrive at the services OEM experience score. Credential is to be submitted for each of the following services: 1. Breach Attack & Simulation	Point 1 = 0.5 Marks Point 2 = 1 Mark Max Marks – 8 Marks

S.No.	Criteria	Scoring
	2. Continuous Automated Red Teaming services 3. Attack surface management 4. Phishing simulation 5. Either Digital Risk Management Services, OR both Anti-Phishing and Brand Protection & Monitoring Services 6. Dark web monitoring 7. Threat Intelligence feed 8. Threat Hunting services Category: a. Point 1: 1 Client b. Point 2: ≥2 Clients	
7	Technical presentation A presentation to be made by the bidder covering the following aspects (but not limited to): a. Capability demonstration by the bidder b. Understanding of Scope of work & terms of the RFP c. Proposed Approach and Methodology for implementation d. Approach & methodology for providing Managed Security Services (MSS) to run Security Operation Centre (SOC) services e. Solution Description, Functionality, Architecture & Deployment model, Posture of proposed architecture f. Resource Deployment plan, Implementation Plan g. OEM Proposed project detailed Go-Live timelines for each solution with milestones. h. Bidder to demonstrate a relevant AI/ML capability use case, playbooks, models etc. All eligible bidders will be required to make presentations. The bank will schedule presentations, and the time and location will be	Max Marks 15

S.No.	Criteria	Scoring
	communicated to the bidders. Failure of a bidder to complete a scheduled presentation to the bank may result in rejection of the proposal. As part of the technical evaluation, all qualified bidders shall be required to make a detailed Technical Presentation to the Evaluation Committee. Technical presentation and Responses provided during the session will be considered part of the Technical Bid and are contractually binding. Bank reserves the right to perform the reference check through VC/Reference call/site visit/other mode of communication as deemed necessary by the evaluation team.	

10.4 Commercial Evaluation Criteria

The commercial bid of only Eligible & technically qualified bidders shall be opened. These qualified bidders as per evaluation process will participate in Commercial evaluation process.

The Commercial offers of only those Bidders, who are short-listed after technical evaluation, would be opened. The format for quoting commercial bid is set in Appendix 2-Commercial Bill of Material. The commercial offer should consist of comprehensive cost for required solution. The bidder must provide detailed cost breakdown, for each category mentioned in the commercial bid.

The Bank reserves the right to proceed with the commercial bid opening and subsequent procurement process even if only one bidder qualifies the eligibility evaluation criteria stipulated under this RFP. Such a decision may be taken by the Bank at its sole discretion, considering the criticality of the requirement, urgency of implementation, business continuity needs, operational considerations, or any other factors deemed relevant by the Bank. The decision of the Bank in this regard shall be final, conclusive, and binding on all bidders.

The commercial offer should consist of comprehensive cost for all the components in the format provided in Appendix 2: Commercial Bill of Material

Bidder must provide detailed cost breakdown, for each and every categories/line items mentioned in the commercial bid.

The BANK will determine whether the Commercial Bids are complete, unqualified and unconditional. Omissions, if any, in costing any item shall not entitle the firm to be compensated and the liability to fulfil its obligations as per the Scope of the RFP within the total quoted price shall be that of the Bidder.

The bidder quoting the lowest evaluated Total Cost of Ownership (TCO), as determined by the Bank in accordance with the Commercial Bid format and evaluation criteria specified in this RFP, shall be ranked as L1 (Lowest Bidder). Award of Contract shall be considered for the bidder ranked L1, subject to compliance with all terms and conditions of the RFP.

The determination of the evaluated TCO and the ranking of bidders shall be final and binding on all bidders. The Bank reserves the right to seek clarifications, verify arithmetic accuracy, correct computational errors, and re-compute the evaluated TCO wherever required. In the event of any discrepancy between unit rates and total prices, the unit rates shall prevail, and the evaluated TCO shall be revised accordingly.

<u>Commercial Bid Evaluation Considerations:</u>
Commercial bid valuation shall be considered as below in case of any kind of discrepancy:

1. If there is a discrepancy between words and figures, the amount in words shall prevail
2. If there is a discrepancy between percentage and amount, the amount calculated as per the stipulated percentage basis shall prevail
3. Where there is a discrepancy between the unit rate and the line-item total resulting from multiplying the unit rate by quantity, the unit rate will govern unless, in the opinion of bank, there is an obvious error such as a misplacement of a decimal point, in which case the line-item total will prevail
4. Where there is a discrepancy between the amount mentioned in the bid and the total line-item present in the schedule of prices, the amount obtained on totaling the line items in the Bill of Materials will prevail
5. The amount stated in the correction form, adjusted in accordance with the above

procedure, shall be considered as binding, unless it causes the overall price to rise, in which case the bid price shall prevail

6. If there is a discrepancy in the total, the correct total shall be arrived at by bank.
7. In case the bidder does not accept the correction of the errors as stated above, the bid shall be rejected.
8. At the sole discretion and determination of the bank, the bank may add any other relevant criteria for evaluating the proposals received in response limited to the terms defined in this RFP without material impact.
9. Bank may, at its sole discretion, decide to seek more information from the respondents in order to normalize the bids. However, respondents will be notified separately if such normalization exercise as part of the technical evaluation is resorted to.
10. All liability related to non-compliance of minimum wages requirement and any other law will be responsibility of the bidder.
11. The bank shall not incur any liability to the affected bidder on account of such rejection.
12. The commercials will be calculated till two decimal points only. If the third decimal point is greater than .005 the same shall be scaled up else, it shall be scaled down to arrive at two decimal points. Bank will make similar treatment for 4th or subsequent decimal point to finally arrive at two decimal points only.

11 Right to Reduce / Descope Solution Components Prior to Award – Clause Stands Deleted.

12 PAYMENT TERMS

The selected Bidder will have to submit the documents (Delivery challans with all the part codes of OEM which shall be reconciled with BOM) at the Bank's office along with a request letter for payment. No advance payment will be made. Payment will be made in Indian Rupees only. All taxes to be paid will be subject to GST applicability. TDS will be applicable.

All out of pocket expenses, travelling, boarding and lodging expenses for the entire term of this RFP and subsequent agreement is included in the amount and service provider shall not be entitled to charge any additional cost on account of any items or services or by way of any out-of-pocket expense, including travelling, boarding, and lodging etc.

Bank will release payment within 30 days from the date of receipt of invoice. In case of dispute, payment will be made within 30 working days of the resolution of disputes.

12.1 Product (Software) Cost

Product Cost is defined as the sum of One time Product License Cost and One time implementation cost of the respective product

#	Items	Milestone	Percentage
1.	Product License Cost	On successful delivery of the licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware. The Bidder is required to submit the required to submit the following: • Delivery proof • OOTB Installation Proof • Invoice of the Product	50%

#	Items	Milestone	Percentage
		On successful UAT Signoff of the respective product	20%
		On successful Go-live of the respective product	30%
2	Product Implementation Cost	On Successful installation of OOTB product on the sourced hardware and handing over the environment with OOTB product to Bank	20%
		On successful UAT Signoff of the respective product	50%
		On successful Go-live of the respective product	20%
		Within 3 months of successful Go-live	10%
3.	Subscription Cost (One time license Cost)	On successful delivery of the Licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware. The Bidder is required to submit the required to submit the following: • Delivery proof • OOTB Installation Proof • Invoice of the Product	50%
		On successful UAT Signoff of the respective product	20%
		On successful Go-live of the respective product	30%

*No factors, under any circumstances, shall affect the bank's services, infrastructure, solutions, or the committed costs and SLAs as defined in the RFP.

Note:

- The payment milestones specified under Product License Cost and Subscription Cost shall be applicable to the respective licensing model proposed by the bidder.
- Irrespective of whether the bidder proposes a Perpetual Licensing Model, Subscription Licensing Model, or any other OEM-supported licensing model, the quoted Product License Cost/Subscription Cost, as applicable, shall include the applicable software licence/subscription together OEM warranty, support, updates, upgrades, patches, bug fixes, and maintenance, in accordance with Section 7.11 (Warranty, ATS & AMC) and other provisions of the RFP.
- For Perpetual or any other non-subscription licensing model, the Annual Technical Support (ATS) charges shall be quoted separately in the Commercial Bill of Material.
- For the Subscription Licensing Model, the Subscription Renewal Charges for Year-4 and Year-5 shall be quoted separately in the Commercial Bill of Material and shall be payable from the fourth year onwards.
- Accordingly, the payment milestones and the Commercial Bill of Material prescribed in the RFP are applicable to all licensing models.

12.2 OEM Services Cost

S. No	Items	Milestone	Percentage
1	OEM Services Cost	Payable in arrears post providing the service	Quarterly in arrears
	Architecture Assessment	Submission of Report to Bank along with detailed presentation to bank's senior management on yearly basis	In arrears

Payment will begin after sign-off of the services configurations and the bank has started using the same for its intended use.

12.3 Hardware Cost

(Hardware cost is defined as the sum of One time Hardware Cost, and Installation cost of the respective hardware)

S. No.	Items	Milestone	Percentage
1	Appliance Cost	On successful Delivery of the Appliance which would be considered delivered once the solution (with OOTB features) is made available for view and review of the bank. The Bidder is required to submit the required to submit the following: • Delivery proof • OOTB Installation Proof • Invoice of the Product	50%
		On successful UAT Signoff of the respective product	20%
		On successful Go-live of the respective product	30%
2.	Hardware Cost (Other than Appliances)	Delivery of hardware and submission of invoice with Proof of Delivery and other documents of the hardware supplied. Bank may at its discretion verify the details before releasing the payment (This verification, if required, shall be completed within 1 month of delivery of the hardware on the bank's premises).	70%
		On successful installation of proposed solutions on the hardware - 50% of the sought product/solutions	15%
		On successful installation of remaining proposed solution on the hardware – remaining 50% of the sought product/solutions	15%

OOTB – Out of the Box (The features marked as standard feature by the OEMs of the respective solution in the compliance sheets)

12.4 ATS/subscription cost & AMC Cost

(ATS/ subscription cost & AMC Cost – Annual ATS & AMC Support of the respective software & hardware)

S. No	Items	Milestone	Percentage

1	ATS/ Annual Subscription & Appliance AMC Cost	ATS/ Annual Subscription Cost	Annually in Advance: Upon submission of a Bank Guarantee equivalent to 110% of the annual subscription/Annual technical cost of the respective product, valid for the applicable subscription period; or Quarterly in Arrears
		Appliance AMC	Annually in advance, upon submission of a Bank Guarantee equivalent to 110% of the annual AMC amount of the respective product, or quarterly in arrears, as per the terms and conditions of the Contract.

12.5 Facility Management (FM) Cost:

(FM manpower Support for maintaining and managing the proposed solution, services and complying with the terms of the RFP)

S. No	Items	Milestone	Percentage
1	FM Manpower Cost	Submission of SLA report and Submission of attendance record/register of Onsite resources on Quarterly basis	Quarterly in arrears

12.6 Other Cost

Cost for the respective line items in the Bill of Material

S. No	Items	Milestone	Percentage
1	Other Cost	Payable in arrears	After completion of respective activity

Note:

a. Annual Maintenance Contract (AMC)/ Annual Technical Support (ATS) includes all appliance, software, applications, component, services deployed/required to meet the required terms of the RFP
b. Activities need to be carried out simultaneously for speedy production roll out as per Bank's expectations and standards. Bank may involve third parties at various stages for review, verification of completeness of NextGEN SOC Security setup and onsite & offsite activities etc. without obtaining permission from the bidder & OEMs

Note:- The Bidder shall submit, prior to the release of each payment during the O&M phase, an undertaking signed by respective OEM confirming that there are no outstanding or overdue amounts payable by the Bidder in respect of the proposed solution(s) and services under this RFP.

The Bidder shall ensure that any dispute, claim or outstanding payment between the Bidder and the OEM(s) shall not, under any circumstances, adversely affect the continuity, availability, support, performance, licensing, maintenance, upgrades or any other Services provided to the Bank during the entire contract period.

13 SERVICE LEVELS & PENALTIES

13.1 Service Level Agreement

The successful bidder shall comply with the following Service Level Requirements throughout the contract period-

1. The successful bidder shall enter into a Service Level Agreement (SLA) incorporating all applicable terms and conditions of this RFP for maintaining the required uptime and providing support services, including onsite support, throughout the contract period.
2. The bidder and the OEM shall be jointly responsible for the maintenance, configuration, performance, and fault-free operation of the entire supplied infrastructure, including hardware, software, operating systems, databases, and related components, during the warranty, AMC, ATS, and FMS periods, as applicable.
3. Any technical issues, faults, or malfunction affecting the installed solution, including bidder's provided hardware, software, operating systems, databases, firmware, BIOS, or related components, shall be attended to on a priority basis and shall be covered under the applicable warranty, AMC, ATS, and FMS.
4. The bidder should maintain the guaranteed minimum uptime for all systems and solutions supplied under this RFP to prevent business disruption, service degradation, or data unavailability. Uptime shall be measured and calculated on a monthly basis.
5. Incidents, faults, or breakdowns may be reported by the Bank through telephone, email, service desk ticketing system, or any other mutually agreed communication mechanism.
6. For SLA and penalty calculations, downtime shall be measured from the time the Bank/bank's appointed vendor reports the incident to the bidder until the time the bidder notifies the Bank that the issue has been resolved, and normal services have been restored, subject to verification by the Bank.
7. Any applicable penalties shall be deducted from the quarterly AMC, ATS, or FMS payments. If the penalty amount cannot be recovered through such payments, the Bank reserves the right to recover the amount by invoking the Performance Bank Guarantee (PBG).
8. Failure to provide support services in accordance with the SLA requirements, including the required support coverage and service quality specified in this RFP, may result in bank levying penalty, termination of the contract, or any other action deemed appropriate by the Bank, without prejudice to its other contractual rights and remedies.
9. The bidder shall conduct preventive maintenance activities at least once every quarter and perform breakdown maintenance as required, without adversely affecting the Bank's normal operations. Such activities shall support the maintenance of the required up-time on a 24x7x365 basis.
10. The bidder shall provide support services on a 24x7x365 basis and, whenever required, perform activities beyond normal business hours, including weekends and holidays.
11. In addition to maintaining the required uptime, the bidder shall adhere to the incident response, restoration, and resolution timelines specified in this RFP for all hardware, software, system software, and related component failures
12. Uptime shall be calculated as follows:

$$\text{Uptime (\%)} = \frac{\text{Total Hours in the Month} - \text{Downtime Hours in the Month}}{\text{Total Hours in the Month}} \times 100$$

Planned or scheduled downtime approved in advance by the Bank shall be excluded from uptime and penalty calculations. The Bank shall make payments after deducting any applicable LD & SLA penalties.

13. If any critical component of the supplied solution becomes non-functional, the bidder and OEM shall, within four (4) hours of incident reporting, either:
    a) repair the defective component,
    b) replace it with a new equivalent component, or
    c) provide a standby replacement at no additional cost to the Bank.

The bidder shall maintain adequate inventory of spare and standby components to meet this requirement

14. If the bidder fails to restore service or provide a replacement/standby component within the stipulated four (4) hour period, the Bank may undertake or arrange remedial measures at the bidder's risk and cost, without prejudice to any other rights and remedies available under the contract.
15. The bidder shall comply with the Bank's security policies, audit requirements, and applicable regulatory guidelines. The bidder shall also implement all necessary operating systems, firmware, BIOS, security, and related updates or patches during the contract period at no additional cost to the Bank.
16. For all incidents related to the supplied solution, the bidder shall submit a Root Cause Analysis (RCA) report issued by the respective OEM within three (3) working days from the date of incident resolution. A penalty of ₹20,000 per calendar day shall be levied for any delay in submission of the RCA report beyond the defined timelines.
17. Total penalties due Service level and liquidated damages shall not exceed 10% of the Total contract value

The bidder shall classify, respond to, and resolve incidents in accordance with the following severity levels and associated Service Level requirements

Level Classifications
Criticality Table

Severity Level	Classification Criteria	Response Time	Resolution Time
Critical / High	Any incident resulting in one or more of the following: 1. Complete or significant disruption preventing users from performing their business operations. 2. Failure of any production component of the proposed solution, IT infrastructure, or associated services. 3. Security incidents affecting confidentiality, integrity, or availability of systems or data. 4. No acceptable workaround or manual process is available. 5. Potential financial, regulatory, operational, or reputational impact on the Bank. 6. Failure or unavailability of critical infrastructure components including, but not limited to: i. Application servers ii. Web servers iii. Database servers/appliances iv. Solution servers/appliances v. Storage vi. Backup Infrastructures vii. Network components supplied under the contract	Within 15 minutes (24x7x365)	Within 45 Minutes
Key / Medium	Any incident resulting in one or more of the following: 1. An incident not classified as Critical, for which a temporary workaround is available.	Within 15 minutes (24x7x365)	Within 90 Minutes

Severity Level	Classification Criteria	Response Time	Resolution Time
	2. Degradation or non-availability of the proposed solution infrastructure affecting performance, functionality, or query processing as defined in the RFP. 3. Severe functional restrictions experienced by users, irrespective of the cause. 4. Issues affecting key support environments a.		
Significant / Low	Any incident resulting in one or more of the following: 1. An incident not classified as Critical or Medium and for which an acceptable workaround is available. 2. Moderate functional restrictions with limited business impact. 3. No impact on normal business processing or critical operations. 4. Issues affecting equipment, systems, or applications that do not impact day-to-day operations. 5. Any other infrastructure or component not covered under the Critical or Medium categories.	Within 15 minutes (24x7x365)	Within 150 Minutes

Service Levels

1. Service Level monitoring shall include both Availability Metrics and Performance Metrics for all solutions, infrastructure, software, appliances, and services supplied under this RFP.
2. The bidder shall submit Monthly Availability Reports and Quarterly Availability Reports to the Bank. These reports shall be reviewed by the Bank to assess compliance with the agreed Service Levels.
3. The Monthly Availability Report shall be submitted within the timelines specified by the Bank and shall, at a minimum, include:
    a. System and service availability statistics;
    b. Details of all incidents reported during the reporting period;
    c. Incident classification and severity levels;

d. Response and resolution times;
e. Downtime analysis;
f. SLA compliance status;
g. Root cause summaries and corrective actions taken; and
h. Any other information reasonably required by the Bank

4. Performance measurement shall be carried out through reports, audits, monitoring tools, or any other mechanism deemed appropriate by the Bank. The bidder shall provide all necessary monitoring and reporting tools required for measuring service performance.
5. Performance reports may include, but are not limited to:
    a. Resource utilization reports;
    b. System performance reports;
    c. Application response time reports;
    d. Capacity utilization reports;
    e. Network performance reports;
    f. Security monitoring reports; and
    g. Any other reports required for assessing compliance with the Service Levels
6. The Bank, or any agency authorized by the Bank, may conduct periodic or ad-hoc audits to verify compliance with the Service Levels, security requirements, regulatory obligations, and contractual commitments. The bidder shall provide all necessary assistance, access, logs, reports, and supporting information required for such audits
7. Any non-compliance identified through reports, audits, or monitoring activities shall be addressed by the bidder within the timelines prescribed by the Bank, without any additional cost to the Bank
8. Penalties shall be calculated only for service degradation or downtime attributable to bidder.
9. The tools to perform the audit will need to be provided by Bidder. Audits will normally be conducted on a regular basis or as required by BANK and will be performed by BANK or BANK appointed third party agencies.
10. SLA Monitoring Mechanism
    a. The bidder shall propose a comprehensive SLA monitoring and reporting mechanism for measuring, tracking, and reporting compliance with the Service Levels defined under this RFP.
    b. The proposed monitoring mechanism, including dashboards, reports, metrics, and measurement methodology, shall be subject to review and approval by the Bank.
    c. The bidder shall provide the Bank with access to relevant tools, dashboards, logs, and reports required to independently verify SLA compliance and service performance.

d. The Bank reserves the right to validate, audit, or independently measure the Service Levels through its own tools, processes, or authorized third-party agencies. In the event of any discrepancy, the Bank's determination shall prevail unless the bidder provides satisfactory evidence to the contrary.

For the purpose of SLA penalty computation and related calculations, the Monthly Maintenance Cost (MMC) shall be calculated as follows:

Monthly Maintenance Cost =	Total FM (O&M) Manpower Cost+Total AMC Cost of Infrastructure/Appliances+Total ATS or Subscription Cost of Software/Tools 60

Quarterly Maintenance Cost =	Total FM (O&M) Manpower Cost+Total AMC Cost of Infrastructure/Appliances+Total ATS or Subscription Cost of Software/Tools 20

Availability Measurements

Level	Type of Infrastructure	Measurement	Minimum Service Level	Penalty
Cyber Security Solutions and IT Infrastructure (HCI/Virtualization, OS, DB, IT Components Etc.) for Cyber security solutions	Proposed Infrastructure & Systems	Availability of each solution, Infrastructure Elements & Systems, any individual component	The minimum monthly uptime requirements are as follows: • Hybrid solution, comprising On-Cloud / SaaS components and On-Premises components, where the On-Premises components are deployed in N+N Active-Active / HA configuration – 99.99% • Hybrid solution, comprising On-Cloud / SaaS components and On-Premises components,	For every 0.05% or part thereof drop in service levels penalty will be 1% of the Monthly Maintenance Cost The Calculation of penalty will happen based monthly performance data as received

Level	Type of Infrastructure	Measurement	Minimum Service Level	Penalty
			where the On-Premises components are deployed in Standalone configuration – 99.90% • On-Premises solution/components/modules deployed in N+N Active-Active / HA configuration - 99.99% • Standalone On-Premises solution – 99.90%	

- Availability Service Levels shall be measured and evaluated on a monthly basis.
- The bidder's performance against the prescribed Availability Service Levels shall be assessed monthly for each applicable solution, service, appliance, software component, or system covered under the scope of this RFP, in accordance with the minimum service levels specified in the Availability Measurement Table.
- An Availability Service Level Default shall be deemed to have occurred if the bidder fails to achieve the prescribed Minimum Availability Service Level for any applicable service, solution, or component during a given month.
- Availability measurements and corresponding SLA compliance assessments shall be based on the monthly performance reports and downtime records validated by the Bank.

Services SLAs:

Service Area	Service Level	Penalty
Each Proposed Services Uptimes	99.90%	For every 0.05% or part thereof drop in service levels penalty will be 1% of the Monthly Maintenance Cost

Service Area	Service Level	Penalty
		Service level drop below 90%, penalty shall amount to 100% of the Monthly Maintenance Cost
Anti-phishing, Anti-rogue app, anti-malware etc. Brand protection and Monitoring Dark Web Monitoring	**a.** Detection of phishing sites, rogue app, brand abuse, malicious content etc. elaborated in RFP ≥ 85% **b.** Site take-down time for identified Phishing URLs – Resolution within 24 hours **c.** Site take-down time for Brand Abuse – Resolution within 36 hours **d.** Enrichment: Cybercrime – Resolution within 1 Hours **e.** Enrichment: Nation State– Resolution within 1 Hours **f.** Any other (Like Interaction, Ransomware, Malware Reverse Engineering etc.) – Resolution within 1 Hours (From the time of reporting the request / issue through phone call / email / web-based portal)	Non-detection or late detection - Rs. 1 Lakh each for non-detection or late detection of phishing site, anti-rogue, malware, social media, mobile app, etc. Point b to Point f -- Rs.5000/- for every hour beyond resolution time.
Continuous Automated Red Teaming Services Threat Intelligence Feed Threat Hunting Services Phishing Simulation Attack Surface Management Breach Attack & Simulation	• Performing the Activity as pe the defined frequency and/or • Submission of report to the bank	Delay in performing the activity – 1% of monthly maintenance cost per day of delay Delay in submission of the report – 1% of monthly maintenance cost per day of delay The penalties for delay in completion of Exercise and submission of report will be mutually exclusive

The mechanism for monitoring the SLA would need to be proposed by the bidder and agreed by the BANK.

Performance Measurements
Performance Measurements will be made on a monthly basis or as required by BANK.

Service Area	Measurement Criteria	Minimum Service Level	Measurement Method	Penalty
Hardware Utilization	Daily peak utilization of CPU, memory (RAM), network interfaces (NIC), storage I/O, or other critical infrastructure resources exceeds 75% for more than 5 consecutive minutes. Each subsequent block of 5 minutes shall be treated as a separate incident. Where virtual machines (VMs), containers, or similar workloads are deployed, utilization shall also be measured at the individual VM/container level. Utilization of any VM or container shall not exceed 75% for more than 5 consecutive minutes.	100% Compliance	Incident reports, monitoring tools, utilization reports, and Bank audits.	If utilization thresholds are exceeded up to three (3) incidents in a calendar month, a penalty of 1% of the Monthly Maintenance Cost (MMC) shall be levied for each incident. If utilization thresholds are exceeded more than three (3) times in a calendar month, the bidder shall augment, optimize, or otherwise remediate the capacity deficiency at no additional cost to the Bank within three (3) months.
Storage Utilization (Primary, Object, Backup, and Long-Term Storage including	Daily peak storage utilization exceeds 80% for more than 5 consecutive minutes. Each subsequent block of 5	100% Compliance	Incident reports, monitoring tools, utilization reports, and Bank audits.	If utilization thresholds are exceeded up to three (3) incidents in a calendar month, a penalty of 1% of the Monthly Maintenance Cost (MMC) shall be levied for each incident.

Service Area	Measurement Criteria	Minimum Service Level	Measurement Method	Penalty
Appliance Storage and Software-defined storage)	minutes shall be treated as a separate incident.			If utilization thresholds are exceeded more than three (3) times in a calendar month, the bidder shall augment, optimize, or otherwise remediate the capacity deficiency at no additional cost to the Bank within three (3) months.
Disaster Recovery (DR) Instance Availability	Restoration of business operations from the Disaster Recovery site within the defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) following failure or unavailability of the primary site. • RPO: 15 minutes • RTO: 60 minutes	100% Compliance (Instance-wise)	Periodic audits, DR drills, test reports, and Bank verification.	A penalty of ₹10,000 for every 10 minutes or part thereof beyond the stipulated RPO or RTO shall be levied.

Incident Management

Service Level	Description	Measurement Method	Periodicity	MSL	Service Credit / Penalty
Incident Acknowledgement & Ticket Logging	The bidder shall acknowledge all incidents reported through approved channels (service desk, email, phone, monitoring tools, etc.) and generate a unique ticket/reference number.	Number of incidents acknowledged and ticketed within prescribed minutes ÷ Total incidents reported × 100	Monthly	100%	Penalty of INR 20,000 for every delay of 30 minutes or part thereof per incident.

Service Level	Description	Measurement Method	Periodicity	MSL	Service Credit / Penalty
	The ticket number shall be communicated to the Bank within the timelines defined in the Criticality Table				
Incident Response & Resolution Compliance	The bidder shall respond to and resolve all incidents within the applicable response and resolution timelines specified in the RFP, based on incident severity/category.	Number of incidents responded to and resolved within prescribed timelines ÷ Total incidents logged × 100	Monthly	100%	For every 0.5% drop in SLA achievement or part thereof below the MSL, penalty of 0.5% of the monthly ATS/AMC charges.

Management, Reporting and Governance

Service Level	Description	Measurement Method	Periodicity	MSL	Service Credit / Penalty	Remarks
Deployment and Retention of Key Resources	The bidder shall deploy the Key Resources proposed in its bid and shall not replace any Key Resource without prior written approval of the Bank, except in cases of resignation, long-term illness, death, or other reasons acceptable to the Bank.	Number of unauthorized replacements of Key Resources during the contract period.	Contract Period	100%	Penalty of INR 2,00,000 per instance of unauthorized replacement of each Key Resource.	Replacement resource shall possess qualifications and experience equal to or better than the outgoing resource and shall be subject to Bank approval.

Service Level	Description	Measurement Method	Periodicity	MSL	Service Credit / Penalty	Remarks
Manpower Availability	The bidder shall maintain the minimum manpower strength specified in the RFP at all times. Any absence shall be immediately substituted with an equivalent or higher skilled resource.	Actual manpower deployed ÷ Required manpower strength × 100.	Monthly	100%	Any breach of the 100% availability requirement for the mandatory minimum positions and resource counts specified in the RFP shall attract a penalty of INR 25,000 per resource per week or part thereof Penalty shall be applicable from the date of breach until the required manpower strength is restored. The mandatory minimum positions specified under Section 7.12 (Resource Requirement – Minimum Resource Count Deployment) shall be maintained at 100% throughout the	Resource availability shall be calculated monthly based on approved attendance records and deployment reports.

Service Level	Description	Measurement Method	Periodicity	MSL	Service Credit / Penalty	Remarks
					Contract Period. Any vacancy, absence, or shortfall in the mandatory minimum resource count shall be immediately replaced with an equivalent or higher-skilled resource. Failure to maintain the mandatory minimum deployment shall be considered an SLA breach and shall attract penalties as defined below from the date of breach until the required deployment is restored.	
SLA and Operational Report Submission	The bidder shall submit all SLA, performance, operational, compliance and governance reports as prescribed by the Bank.	Number of reports submitted within stipulated timelines ÷ Total reports due.	Monthly	100%	Penalty of INR 20,000 per week or part thereof for each delayed or missed report.	All reports for a calendar month shall be submitted by the 7th day of the subsequent month unless otherwise specified by the Bank. The Bank may modify the reporting requirements during the contract period.

Service Level	Description	Measurement Method	Periodicity	MSL	Service Credit / Penalty	Remarks
Security Device Management and Administration	The bidder shall provide 24x7 monitoring, management, administration, configuration and change management services for all in-scope security solutions and devices.	Number of approved changes executed without error ÷ Total approved changes implemented.	Monthly	100%	Incorrect rule/configuration change: INR 20,000 per instance. Incorrect rule/configuration change resulting in service disruption, security incident, or business impact: INR 30,000 per instance.	Applies to all security devices and solutions covered under the scope of the RFP. All changes shall be implemented only after obtaining requisite approvals from the Bank.

Security Vulnerability Management:

Service Area	Service Level Description	Measurement Method	Periodicity	MSL	Service Credit / Penalty
Version Upgrades, Security Patching and Firmware Updates	The bidder shall implement all OEM-recommended and Bank-approved operating system, database, middleware, application, firmware, security, and hardware patches/upgrades in accordance with the approved Patch and Upgrade Management Calendar. The bidder shall publish a monthly patching and upgrade schedule and obtain necessary approvals prior to	Number of approved upgrades, patches, firmware updates and version updates successfully implemented within the approved timeline ÷ Total upgrades, patches, firmware updates and version updates due during the measurement period × 100.	Monthly	95%	95% and above compliance: No Penalty. Below 95% compliance: Penalty of INR 500 per day per percentage point (or part thereof) below the prescribed MSL, until the pending upgrades/patches are successfully implemented and verified by the Bank.

Service Area	Service Level Description	Measurement Method	Periodicity	MSL	Service Credit / Penalty
	implementation. This SLA shall become applicable one (1) month after Go-Live/Operational Acceptance.				

Management & health checkup:

Service Area	Service Level Description	Measurement Method	Periodicity	MSL	Service Credit / Penalty
OEM Governance and Review	The bidder shall ensure participation of the respective OEM(s) in periodic review meetings, health checks, architecture reviews, performance reviews, and issue resolution discussions as required by the Bank and specified in the RFP.	Number of OEM review engagements conducted as scheduled ÷ Number of OEM review engagements required.	As Required	100%	Failure to conduct the scheduled OEM review or engagement shall attract a penalty of INR 2,00,000 per affected solution per day or part thereof from the scheduled date of the review until completion of the OEM engagement.
OEM Support Case Management	The bidder shall proactively manage and coordinate with OEMs for resolution of product defects, bugs, vulnerabilities, and technical issues. All OEM support tickets shall be tracked and escalated appropriately until closure or implementation of an acceptable	Number of OEM support cases resolved within the prescribed timeline ÷ Total OEM support cases due for closure.	Monthly	100%	For OEM support cases remaining unresolved beyond 14 calendar days without a Bank-approved workaround, penalty of 1% of the applicable monthly ATS/AMC/Managed Services charges per week or part thereof until closure.

Service Area	Service Level Description	Measurement Method	Periodicity	MSL	Service Credit / Penalty
	workaround approved by the Bank.				
Compliance with RBI, CERT-In and Regulatory Advisories	The bidder shall assess, implement and ensure compliance with all applicable RBI, CERT-In, Government of India, regulatory, statutory, and security advisories within the timelines prescribed by the issuing authority or as directed by the Bank.	Number of applicable advisories complied with within prescribed timelines ÷ Total applicable advisories.	Monthly	100%	Compliance within the stipulated timeline – No Penalty. Delay in compliance beyond the prescribed due date shall attract a penalty of 0.5% of the applicable monthly contract value per day of delay, subject to the overall penalty cap specified in the RFP.

Audit (IS & VAPT and other internal/external audit) Gaps-The Resolution time should begin from the date/time being notified by the bank

Service Area	Observation Severity	Resolution Timeline	Service Level Requirement	Penalty
IS Audit / VAPT / Security Audit Observation Closure	Highly Critical	Within 6 hours from identification of the vulnerability	100% closure within prescribed timeline	INR 50,000 per observation per 6 hours or part thereof beyond the prescribed timeline until closure and acceptance by the Bank.
	Critical	Within 24 calendar hours from issuance of the audit report or identification of the vulnerability	100% closure within prescribed timeline	INR 20,000 per observation per day or part thereof beyond the prescribed timeline until closure and acceptance by the Bank.
	High	Within 7 calendar days from issuance of the audit report or identification of the vulnerability	100% closure within prescribed timeline	INR 10,000 per observation per day or part thereof beyond the prescribed timeline until closure and acceptance by the Bank.

Service Area	Observation Severity	Resolution Timeline	Service Level Requirement	Penalty
	Medium	Within 15 calendar days from issuance of the audit report or identification of the vulnerability	100% closure within prescribed timeline	INR 5,000 per observation per day or part thereof beyond the prescribed timeline until closure and acceptance by the Bank.
	Low	Within 45 calendar days from issuance of the audit report or identification of the vulnerability	100% closure within prescribed timeline	INR 3,000 per observation per day or part thereof beyond the prescribed timeline until closure and acceptance by the Bank.

Bidder is required to submit the compliance document confirming that the identified gaps have been closed.

13.2 Penalties

For the purpose of this RFP, the total penalties as per LD & SLA will be subject to a maximum of 10% of the overall contract value.

Liquidated Damages

Supply & Delivery

Please refer to section 14.19 for LD on Supply & Delivery

Installation & Implementation

Delay in delivery, installation, configuration, integration, testing, commissioning, migration, implementation, Go-Live, or any project milestone approved by the Bank., the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 1% per week or part thereof of the respective Product Cost subject to maximum deduction of 10% of the total contract value, until actual delivery and implementation as per related clauses mentioned in RFP.

* Product Cost = Product License/Subscription Cost + Implementation + Configuration + Integration + Migration + Commissioning Cost.

If the LD due to Implementation of the respective product cost/existing product cost reaches 25% of the implementation cost of the respective product/services, the bidder is required to replace the product/services.

Once the maximum deduction is reached, the Bank may consider termination of the Contract at its discretion.

In the event of Bank agreeing to extend the date of delivery at the request of successful bidder(s), it is a condition precedent that the validity of Bank guarantee shall be extended by further period as required by Bank immediately. Failure to do so will be treated as breach of contract.

13.3 At-Risk Amount

The monthly At-Risk Amount (ARA') shall be 15% of the estimated monthly payout of the respective month.

14 TERMS AND CONDITIONS

14.1 Assignment & Subcontracting

1. The selected bidder shall not subcontract/JV/Consortium or permit anyone to perform any of the work, service or other performance required under the contract (excluding Proposed OEM personnels). All bidder's personnel proposed for the bank shall be on bidder's Payroll. Bank will seek relevant documentation from the bidder to validate the same.
2. If the Bank undergoes a merger, amalgamation, takeover, consolidation, reconstruction, change of ownership, etc., this tender shall be assigned to the new entity, and such an act shall not affect the rights of the Agency under this tender.
3. All Bidder's personnel deployed on the project shall be on the Bidder's payroll. The Bidder shall submit the relevant EPFO and ESIC details/documents of each of the personnel to the Bank for verification of their employment status.

14.2 Right to Alter quantities

The bank reserves the right, at the time of award of contract and/or during the currency of the contract, to increase or decrease the quantity of goods, licenses, subscriptions, appliances, equipment, services, implementation effort, support services, or any line item covered under the contract by up to twenty-five percent (25%) of the quantities specified in the RFP/Contract, without any change in the unit prices, terms and conditions, technical specifications, delivery schedule, warranty obligations, support commitments, or any other contractual conditions.

The Bidder/Vendor shall be bound to accept such variation and execute the order at the same rates and on the same terms and conditions as agreed under the contract.

14.3 Delays in the Bidder's Performance

The bidder must strictly adhere to the schedule, as specified in the purchase contract/purchase order, executed between the Parties for performance of the obligations, arising out of the purchase contract and any delay in completion of the obligations by the Bidder will enable Bank to resort to any or both of the following:

1. Claiming Liquidated Damages
2. Termination of the purchase agreement fully or partly and claim liquidated damages.
3. Execution of Bid Declaration Form / Invoking EMD or Performance Bank Guarantee

14.4 Jurisdiction

Jurisdiction: It is hereby agreed between the parties that any suit or legal proceedings to enforce the rights of either party under this Agreement shall be instituted and tried by a competent court in the city of Delhi only.

14.5 Dispute Resolution

If any dispute, difference or claim arises between the parties hereto in connection with the validity, interpretation, implementation or alleged breach of the terms of this Agreement or anything done or omitted to be done pursuant to this Agreement, the Parties shall attempt in the first instance to resolve the same through negotiation.

If no settlement to dispute(s) or difference (s) can be reached through amicable negotiation between the Parties within 30 days of such reference, the Parties shall approach the appropriate Court of Law. However, upon mutual consultation, the Parties may also have an option to refer the dispute(s) or difference(s) for settlement by Arbitration.

If the parties mutually opt for Arbitration, the same shall be conducted as follows:

1. There shall be a sole Arbitrator as mutually appointed by the Parties as per the provisions of The Arbitration and Conciliation Act, 1996 and subsequent modifications thereon.
2. If the parties are unable to appoint a sole Arbitrator on mutual basis, then each Party shall nominate one Arbitrator each, who shall jointly appoint the third Arbitrator (umpire). The majority of such Arbitrators shall be final and binding on the parties.
3. The Proceedings shall be conducted in accordance with the provisions of Arbitration and Conciliation Act, 1996, or any statutory modification or re-enactment thereof for the time being in force.
4. The costs of the Arbitration shall be borne equally by both Parties.
5. Any arbitration shall be confidential and neither you nor the bank may disclose the existence, content or results of any arbitration, except as required by law or purpose of enforcing the arbitration award.
6. The arbitration proceedings shall be in English. The place of Arbitration shall be Delhi and Courts at Delhi shall have exclusive jurisdiction over the matters covered.

If the dispute is not resolved through negotiation or arbitration in 30 (thirty) days after commencement of discussions, then, the parties shall be at liberty to approach competent court of law at Delhi for adjudication of the disputes.

Cost of Arbitration and fees of the Arbitrator(s). The concerned parties shall bear the cost of arbitration equally. The cost shall inter-alia include fees of the Arbitrator. Further, the fees payable to the Arbitrator shall be governed by instructions issued on the subject by the Bank and/ or the Government from time to time, in line with the Arbitration and Conciliation Act, irrespective of the fact whether the Arbitrator is appointed by the Bank or the Government under this clause or by any court of law unless directed explicitly by Hon'ble court otherwise on the matter.

14.6 Notices

Notice or other communications given or required to be given under the contract shall be in writing and shall be faxed/e-mailed followed by hand-delivery with acknowledgement thereof or transmitted by pre-paid registered post or courier.

Any notice or other communication shall be deemed to have been validly given on date of delivery if hand delivered & if sent by registered post than on expiry of seven days from the date of posting.

Publicity

Any publicity by the selected Service Provider in which the name of the Bank is to be used should be done only with the explicit written permission of the Bank.

14.7 Legal Compliance

The successful bidder hereto agrees that it shall comply with all applicable union, state and local laws, ordinances, regulations and codes in performing its obligations hereunder, including the procurement of licenses, permits and certificates and payment of taxes where required. The Successful bidder shall maintain all proper records, particularly but without limitation accounting

records, required by any law, code, practice or corporate policy applicable to it from time to time including records, returns and applicable documents under the Labour Legislation

14.8 Digital Personal Data Protection Compliance

The successful bidder shall comply with all applicable provisions of the Digital Personal Data Protection Act, 2023 and any rules, regulations, or guidelines issued thereunder while collecting, processing, storing, or handling any personal data in connection with this Agreement. The Successful bidder shall implement appropriate technical and organizational security measures to ensure protection of personal data against unauthorized access, disclosure, alteration, or loss. The successful bidder shall immediately notify the Bank of any actual or suspected data breach involving personal data. The successful bidder shall ensure that personal data is used solely for the purposes of performance of the contract and shall not disclose the same to any third party without prior written consent of the Bank. The successful bidder shall indemnify and hold the Bank harmless against any loss, liability, penalty, or damage arising out of any breach or non-compliance with the Digital Personal Data Protection Act, 2023.

1. The successful bidder shall assist the Bank in complying with obligations relating to Data Principal Rights such as access, correction, erasure of data, and grievance redressal under the Act.
2. The successful bidder shall not engage any sub-contractor or sub-processor for processing personal data without prior written permission of the Bank.
3. Upon termination or expiry of the contract, the successful bidder shall return or securely delete all personal data and confirm the same to the Bank.

The successful bidder undertakes not to keep this data with its company after the end of this agreement. This clause will outlive the agreement date. The successful bidder shall sign a Non-disclosure Agreement as stated in the Agreement.

14.9 Non-Disclosure Agreement

The Service Provider shall take all necessary precautions to ensure that all confidential information is treated as confidential and not disclosed or used other than for the purpose of project execution. Service Provider shall suitably defend, indemnify Bank for any loss/damage suffered by Bank. The Service Provider shall have to sign a Non-Disclosure Agreement on stamp paper. No media release, public announcement or any other reference to the agreement or any program there under shall be made without the written consent from the Bank. Reproduction of this agreement, without the prior written consent of the Bank, by photographic, electronic or other means is strictly prohibited.

14.10 Solicitation of Employees

Both parties agree not to hire, solicit, or accept solicitation (either directly, indirectly, or through a third party) for their employees directly involved in this contract during the period of the contract and one year thereafter, except as the parties may agree on a case-by-case basis. The parties agree that for the period of the contract and one year thereafter, neither party will cause or permit any of its directors or employees who have knowledge of the agreement to directly or indirectly solicit for employment the key personnel working on the project contemplated in this proposal except with the written consent of the other party. The above restriction would not apply to either party for hiring such key personnel who (i) initiate discussions regarding such

employment without any direct or indirect solicitation by the other party (ii) respond to any public advertisement placed by either party or its affiliates in a publication of general circulation or (iii) has been terminated by a party prior to the commencement of employment discussions with the other party.

14.11 Authorized Signatory

The selected Bidder shall indicate the authorized signatories who can discuss and correspond with the bank about the obligations under the contract. The selected Bidder shall submit at the time of signing the contract a certified copy of the resolution of their board, authenticated by the company secretary, authorizing an official or officials of the Bidder to discuss, sign agreements/contracts with The Bank, raise invoice and accept payments and also to correspond. The Bidder shall provide proof of signature identification for the above purposes as required by the bank.

14.12 Confidentiality

This document contains information confidential and proprietary to the Bank. Additionally, the Service Provider will be exposed by virtue of the contracted activities to internal business information of the Bank, affiliates, and/or business partners. The Service Provider must undertake that they shall hold in trust any Information received by them under the RFP/ Contract/Service Level Agreement, and the strictest of confidence shall be maintained in respect of such Information. Disclosure of receipt of any part of the aforementioned information to parties not directly involved in providing the services requested could result in the disqualification of the Service Provider, premature termination of the contract, or legal action against the Service Provider for breach of trust. The information provided / which will be provided is solely for the purpose of undertaking the services effectively.

No news release, public announcement, or any other reference to this RFP or any program there under shall be made without written consent of Bank. Reproduction of this Agreement, by photographic, electronic, or other means is strictly prohibited.

The Service Provider must undertake that they shall hold in trust any Information received by them, under the Contract/Agreement, and the strictest of confidence shall be maintained in respect of such Information. The Service Provider has also agree to restrict access and disclosure of Information to such of their employees, agents, strictly on a “need to know” basis, to maintain confidentiality of the Information disclosed to them in accordance with this Clause.

Moreover, Service Provider has to submit Non- Disclosure Agreement along with technical bid as per the format provided in this document.

14.13 Indemnity

The bidder agrees to indemnify and keep indemnified the Bank against all losses, damages, costs, charges and expenses incurred or suffered by the Bank due to or on account of any claim for infringement of intellectual property rights.

The bidder agrees to indemnify and keep indemnified the Bank against all losses, damages, costs, charges and expenses incurred or suffered by the Bank due to or on account of any breach of the terms and conditions contained in this RFP or Service Level Agreement to be executed.

The bidder agrees to indemnify and keep indemnified Bank at all times against all claims, demands, actions, costs, expenses (including legal expenses), loss of reputation and suits which may arise or be brought against the Bank, by third parties on account of negligence or failure to fulfil obligations by the selected bidder or its employees/personnel.

All indemnities shall survive notwithstanding expiry or termination of Service Level Agreement and the bidder shall continue to be liable under the indemnities.

14.14 Make in India

The policy of the Govt. of India to encourage "Make in India" and promote manufacturing and production of goods and services in India, "Public Procurement (Preference to Make in India), Order 2017 and the revised order issued vide GOI, Ministry of Commerce and Industry, Department for Promotion of Industry and Internal trade, vide Order No. P-45021/2/2017-PP (BE-II) dated 19th July 2024 subsequent amendments.

The local supplier at the time of submission of bid shall be required to provide a certificate as per Annexure 7 from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content. The Bank shall follow all the guidelines/ notifications for public procurement.

14.15 Force Majeure

Force Majeure is herein defined as any cause, which is beyond the control of the selected Bidder or The Bank as the case may be which they could not foresee or with a reasonable amount of diligence could not have foreseen and which substantially affect the performance of the contract, such as:-

- Natural phenomenon, including but not limited to floods, droughts, earthquakes, epidemics and pandemics
- Acts of any government, including but not limited to war, declared or undeclared priorities, quarantines and embargos
- Terrorist attack, public unrest in work area
- Provided either party shall within 10 days from occurrence of such a cause, notify the other in writing of such causes. The Bidder or The Bank shall not be liable for delay in performing his/her obligations resulting from any force Majeure cause as referred to and/or defined above. Any delay beyond 30 days shall lead to termination of contract by parties and all obligations expressed quantitatively shall be calculated as on date of termination. Notwithstanding this, provisions related to indemnity, confidentiality survive termination of the contract.
- Unless otherwise directed by the bank in writing, the Bidder affected by force majeure shall continue to perform the obligations under this agreement, which are not affected by the force majeure event and shall take such steps as are reasonably necessary to remove the causes resulting in force majeure and to mitigate the effect thereof.

- As soon as the cause of force majeure has been removed, the Bidder shall notify the Bank and resume the affected activity without delay.
- Notwithstanding the above, the decision of the bank shall be final and binding on the Bidder in the event of force majeure.

14.16 Ownership & Retention of Documents:

The Bank shall own the documents prepared by or for the selected Bidder arising out of or in connection with the Contract.

Forthwith upon expiry or earlier termination of the Contract and at any other time on demand by The Bank, the Bidder shall deliver to The Bank all documents provided by or originating from The Bank / Purchaser and all documents produced by or from or for the Bidder while performing the Service(s), unless otherwise directed in writing by The Bank at no additional cost.

The selected Bidder shall not, without the prior written consent of The Bank/ Purchaser, store, copy, distribute or retain any such Documents.

The selected Bidder shall preserve all documents provided by or originating from The Bank / Purchaser and all documents produced by or from or for the Bidder in the course of performing the Service(s) in accordance with the legal, statutory, regulatory obligations of The Bank /Purchaser in this regard.

14.17 Conflict of Interest:

The Bidder shall disclose to the Bank in writing all actual and potential conflicts of interest that exist, arise or may arise (either for the Bidder or the Bidder's team) in the course of performing the Service(s) as soon as practical after it becomes aware of that conflict.

14.18 Signing of Pre-Contract Integrity Pact:

To ensure transparency, equity, and competitiveness and in compliance with the CVC guidelines, this tender shall be covered under the Integrity Pact (IP) policy of the Bank. The pact essentially envisages an agreement between the prospective bidders/vendor(s) and the Bank committing the persons/officials of both the parties, not to exercise any corrupt influence on any aspect of the contract. The format of the agreement is enclosed as Appendix on stamp paper.

14.19 Liquidated Damages

The Bank will consider the inability of the bidder to deliver or install the equipment & provide the services required within the specified time limit as a breach of contract and would entail the payment of Liquidated Damages on the part of the bidder. The liquidated damages represent an estimate of the loss or damage that the Bank may have suffered due to delay in performance of the obligations (relating to delivery, installation, operationalization, implementation, training, acceptance, warranty, maintenance etc. of the proposed solution/services) by the bidder.

Installation will be treated as incomplete in one / all the following situations:

1. Non-delivery of any component or other services mentioned in the order
2. Non-delivery of supporting documentation
3. Delivery / availability, but no installation of the components and software
4. No integration/ Incomplete Integration
5. Non-Completion of Transition within suggested timeline
6. System operational, but not as per SLA, Timelines and scope of the RFP

If the bidder fails to deliver any or all of the products, systems and services solutions within the time period(s) specified in the Delivery Schedule or installation, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 0.5 percent per week or part thereof of Contract Price subject to maximum deduction of 10% of the total contract value, until actual delivery, installation or performance as per related clauses mentioned in RFP.

Once the maximum deduction is reached, the Bank may consider termination of the Contract at its discretion.

In the event of Bank agreeing to extend the date of delivery at the request of successful bidder(s), it is a condition precedent that the validity of Bank guarantee shall be extended by further period as required by Bank immediately. Failure to do so will be treated as breach of contract.

14.20 Intellectual Property Indemnity:

In the event of any claim asserted by a third party of infringement of copyright, patent, trademark, industrial design rights, etc., arising from the use of the Goods or any part thereof in India as a part of this RFP, the Vendor(s) shall act expeditiously to extinguish such claim. If the Vendor(s) fails to comply and the Bank is required to pay compensation to a third party resulting from such infringement, the Vendor(s) shall be responsible for the compensation to the claimant including all expenses, court costs and lawyer fees. The Bank will give notice to the Vendor(s) of such a claim, if it is made, without delay. The Vendor(s) shall indemnify the Bank against all third-party claims.

14.21 Limitation of Liability

The aggregate liability of bidder in connection with this Agreement, in respect of any claims, losses, costs or damages arising out of or in connection with this RFP/Agreement shall not exceed the total Project Cost. Under no circumstances shall either Party be liable for any indirect, consequential or incidental losses, damages or claims including loss of profit, loss of business or revenue.

The limitations set forth herein shall not apply with respect to:

1. claims that are the subject of indemnification pursuant to infringement of third-party Intellectual Property Right,
2. damage(s) occasioned by the Gross Negligence or Willful Misconduct of Service Provider,
3. damage(s) occasioned by Service Provider for breach of Confidentiality Obligations,
4. Regulatory or statutory fines imposed by a government or Regulatory agency for non-compliance of statutory or regulatory guidelines applicable to the Bank, provided such guidelines were brought to the notice of Service Provider.

"Gross Negligence" means any act or failure to act by a party which was in reckless disregard of or gross indifference to the obligation of the party under this Agreement and which causes injury, damage to life, personal safety, real property, harmful consequences to the other party, which such party knew, or would have known if it was acting as a reasonable person, would result from such act or failure to act for which such Party is legally liable. Notwithstanding the forgoing, Gross Negligence shall not include any action taken in good faith.

"Willful Misconduct" means any act or failure to act with an intentional disregard of any provision of this Agreement, which a party knew or should have known if it was acting as a reasonable person, which would result in injury, damage to life, personal safety, real property, harmful consequences to the other party, but shall not include any error of judgment or mistake made in good faith.

14.22 Order Cancellation

Bank's Right to terminate the entire/ unexecuted part of the Purchase Order on Convenience

1) The Bank reserves its right to cancel the entire unexecuted part of the Purchase Order at any time on its convenience without assigning any reason/s whatsoever.
2) In the event of termination of the Agreement for the Bank's convenience, bidder shall be entitled to receive payment for the Services rendered (delivered) up to the effective date of termination.

Bank's Right to terminate the entire/ unexecuted part of the Purchase Order on Non-Performance/Default

1) The Bank reserves its right to cancel the entire / unexecuted part of the purchase order at any time by assigning appropriate reasons (after providing a cure period of 30 days and thereafter providing a 30 days' notice period). Bank shall serve the notice of termination to the bidder at least 30 days prior of its intention to terminate services because of one of more of the following reasons but not limited to-
   a) Non submission of acceptance of order within 7 days of order.
   b) Excessive delay in execution of orders placed by the Bank.
   c) The selected bidder commits a breach of any of the terms and conditions of the bid.
   d) The bidder goes into liquidation voluntarily or otherwise.
   e) An attachment is levied or continues to be levied for a period of 7 days upon the effects of the bid.
   f) The progress made by the selected bidder is found to be unsatisfactory.
   g) If deductions on account of liquidated Damages/penalties exceeds more than
   h) 10% of the total contract price.
   i) If found blacklisted by any Govt. Department / PSU / other Banks / CERT-In, during contracted period.
   j) Non satisfactory performance of the Project in terms of affecting the Core Systems of the Bank or the Core Business of the Bank and the functioning of the Branches/Offices of the Bank.
2) If the Bank decides to cancel the unexecuted part of the purchase order in whole or in part in the event of one or more of the following conditions:
   a) Delay in delivery of the product installation and Go-Live in the specified period
   b) (Implementation Timelines + Cure Period).
   c) Serious discrepancies are noted in product capability and services.

d) Breaches in the terms and conditions of the Order.

Then the Bank shall have the right to recover from the Bidder any amounts already paid by the Bank in respect of the product (including respective hardware) and services after adjusting for the penalties already levied and recovered by the Bank for that specific product/ service. Further, where the Bidder is able to provide satisfactory evidence that the delay or default was not attributable to the Bidder, such portion shall be excluded from the scope of recovery.

In such case, the Bank may procure on its discretion, upon such terms and in such manner as it deems appropriate, Hardware, software and services similar to those part of the canceled purchase order, and subject to limitation of liability clause of this RFP. However, Bidder shall continue performance of the Contract to the extent not terminated.

3) The Bank reserves its right to invoke the Bank Guarantee/ foreclose the Security Deposit /recover from outstanding amount to the credit of the selected bidder towards the non-performance/non-compliance of the terms and conditions of the contract and/ or to recover the dues payable by the Bidder from any, to appropriate towards damages (as mentioned in Point-1 and Point-2).

Bidder's Obligation on termination

If the Contract is terminated on Non-Performance/contract expiry then –

1) The Bidder shall handover all documents/ executable/ Bank's data or any other relevant information to the Bank in timely manner and in proper format as per scope of this RFP and shall also support the orderly transition to another vendor or to the Bank.
2) During the transition, the Bidder shall also support the Bank on technical queries/support on process implementation or in case of software provision for future upgrades
3) During the transition, the bidder shall continue to provide services as per the terms of the Agreement until a 'New Service Provider' completely takes over the work. During the transition phase, the bidder shall render all reasonable assistance to the new Service Provider within such period prescribed by the Bank, at no extra cost to the Bank, for ensuring smooth switch over and continuity of services, provided where transition services are required by the Bank or New Service Provider beyond the term of this Agreement, reasons for which are not attributable to the bidder, payment shall be made to the bidder for such additional period on the same rates and payment terms as specified in this Agreement.
4) If bidder is in breach of the obligations mentioned in the Point1, 2 and 3, the bidder shall be liable for paying a penalty (as per the SLAs) on demand to the Bank, which may be settled from the payment of invoices or Bank Guarantee for the contracted period or by invocation of Bank Guarantee.

14.23 Consequences of Termination

In the event of termination of the Contract due to any cause whatsoever, [whether consequent to the stipulated term of the Contract or otherwise], the Bank shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the Service(s) which the Bidder shall be obliged to comply with and take all available steps to minimize loss resulting from that termination/breach, and further allow the next successor Bidder to take over the obligations of the erstwhile Bidder in relation to the execution/continued execution of the scope of the Contract.

In the event that the termination of the Contract is due to the expiry of the term of the Contract, a decision not to grant any (further) extension by the Bank , the Bidder herein shall be obliged to provide all such assistance to the next successor Bidder or any other person as may be required and as The Bank may specify including training, where the successor(s) is a representative/personnel of The Bank to enable the successor to adequately provide the Service(s) hereunder, even where such assistance is required to be rendered for a reasonable period that may extend beyond the term/earlier termination hereof. Nothing herein shall restrict the right of The Bank to invoke the Performance Bank Guarantee and other guarantees, securities furnished, enforce the Deed of Indemnity and pursue such other rights and/or remedies that may be available to The Bank under law or otherwise. The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the Contract that are expressly or by implication intended to come into or continue in force on or after such termination.

14.24 Audit by Third Party

The selected bidder (Service Provider), if required, has to get itself annually audited by internal/external empaneled Auditors appointed by the Bank/inspecting official from the Reserve Bank of India or any regulatory authority, covering the risk parameters finalized by the Bank/such auditors in the areas of products (IT hardware/software) and services etc., provided to the Bank and the Service Provider is required to submit such certification by such Auditors to the Bank. The Service Provider and/or his/their outsourced agents/subcontractors (if allowed by the Bank) shall facilitate the same. The Bank can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by the Service Provider. The Service Provider shall, whenever required by the Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by the Bank.

Where any deficiency has been observed during audit of the Service Provider on the risk parameters finalized by the Bank or in the certification submitted by the Auditors, the Service Provider shall correct/resolve the same at the earliest and shall provide all necessary documents related to resolution thereof and the auditor shall further certify in respect of resolution of the deficiencies. The resolution provided by the Service Provider shall require to be certified by the Auditors covering the respective risk parameters against which such deficiencies have been observed.

The Service Provider shall, whenever required by the Bank, furnish all relevant information, records/data to such auditors , inspecting officials of the Bank/Reserve Bank of India , any regulatory authority. The Bank reserves the right to call and/or retain for any relevant material information/reports including auditor review reports undertaken by the service provider (e.g., financial, internal control and security reviews) and findings made on Selected Bidder in conjunction with the services provided to the Bank.

Subject to receipt of prior written notice, all Service provider (s) records/premises with respect to any matters covered by this contract shall be made available to the Bank or its designees and regulators including RBI, at any time during normal business hours, as often as the Bank deems necessary, to audit, examine, and make excerpts or transcripts of all relevant data. Said records are subject to examination. Bank's auditors would execute confidentiality agreement with the Service Provider(s), provided that the auditors would be permitted to submit their findings to the Bank pertaining to the scope of the work, which would be used by the Bank.

14.25 Exit Management

1. Exit Management

Upon expiry or termination of the Agreement, or upon direction of the Bank, the Successful Bidder shall commence Exit Management and fully cooperate with the Bank, its nominated agency and/or Replacement Bidder.

The Successful Bidder shall continue to provide the Services at the agreed SLA levels throughout the transition period, not more than 90 days, until formal acceptance of the transition by the Bank.

2. Exit Management Plan

The Successful Bidder shall provide the Bank with a detailed Exit Management Plan covering, at a minimum, the following:

a) Detailed transition programme, timelines, activities, dependencies and responsibilities of the Bank, Successful Bidder, Replacement Bidder and relevant third parties.
b) Measures to ensure continuity of Services throughout the transition.
c) Transfer of Bank Data, logs, configurations, security content, documentation and other assets required for continued operation of the Services.
d) Knowledge transfer, communication and handover arrangements.
e) Contingent support for a minimum period of one month after completion of transition.
f) Identification and management of technical, operational, contractual and third-party dependencies affecting the transition.

The initial Exit Management Plan shall be submitted by the Successful Bidder within Year 1 of the Contract signing date by the Bank. The plan shall be reviewed and updated annually and shall be finalized within 7 days of any termination or transition notice.

3. Bank Data and Security Data

All data and information provided, uploaded, generated, collected, processed or otherwise made available by or for the Bank in connection with the Services shall remain the sole and exclusive property of the Bank.

This shall include, but not be limited to:

a) Business, transactional and master data.
b) Security logs, raw logs, normalized logs and metadata.
c) Alerts, incidents, cases and audit trails.
d) Investigation records and threat intelligence.
e) Indicators of compromise (IOCs).
f) Reports, dashboards and backups.
g) Configurations and other Bank-specific data.

The Successful Bidder shall provide complete and secure access to, and export of, such Bank Data in open, industry-standard, non-proprietary and usable formats, together with the necessary metadata and relevant configurations.

4. Security Content, Configurations and Intellectual Property Rights

The Successful Bidder shall transfer all Bank-specific security content, detection logic, configurations and operational information that are active or utilized in delivering the Services to the Bank, including, as applicable:

4.1 SIEM and Log Management

Correlation rules, detection rules, custom and modified parsers, normalization rules and schemas, lookup tables, watchlists, threat-hunting queries, dashboards, reports, scheduled searches and risk-scoring configurations.

4.2 Tuning and Whitelisting

False-positive suppression rules, whitelists, exception lists, exclusions, asset-criticality mappings, thresholds and relevant historical tuning information and rationale required for continued effective security monitoring.

4.3 SOAR and Automation

Playbooks, workflows, automation configurations, custom scripts developed for the Bank, API payload templates, webhooks, connectors and integration configurations.

4.4 UEBA

Bank-specific behavioural policies, risk-scoring parameters, peer-group definitions, anomaly-detection configurations and other relevant tuning parameters, to the extent supported by the platform.

4.5 XDR / NDR

Detection policies, custom IOC/IOA rules, exclusion policies, network sensor configurations, device-control policies and Bank-specific response configurations or scripts.

4.6 Threat Intelligence

Bank-specific threat intelligence, curated IOC repositories, watchlists, confidence-scoring configurations and historical threat-hunting or retro-hunting results maintained as part of the Services.

4.7 Other Security Content

Any other Bank-specific security rules, policies, configurations, detection logic or operational artefacts required for the continued operation of the Services.

4.8 Format of Transfer

Bank Data and logs shall be provided in open, industry-standard and non-proprietary formats.

Platform-specific security content and configurations shall, wherever technically supported, be provided in:

i) Native platform export format suitable for re-import into the same platform; and

ii) Human-readable functional documentation describing data sources, relevant log fields, conditions, thresholds, detection logic, dependencies and response actions, and in vendor-neutral formats such as Sigma or YARA, wherever applicable.

The Successful Bidder shall not withhold any Bank-specific detection rule, parser, configuration, playbook or security content on the ground that such content is proprietary or constitutes the Bidder's background IP where such withholding would prevent or materially impair continuity of the Bank's security operations.

The Successful Bidder shall provide the Bank with the necessary rights to retain, use and modify such Bank-specific security content and configurations for the continued internal security operations of the Bank, including through its Replacement Bidder, subject to applicable third-party licensing restrictions.

5. No Lock-in or Reseller Constraints

The Successful Bidder shall not impose any technical, contractual or commercial lock-in or restriction that prevents or materially delays the Bank from:

a) Switching service providers or billing partners.

b) Dealing directly with cloud service providers.

c) Migrating Bank Data, configurations, security content or other Bank-specific assets to another service provider, cloud environment or the Bank's on-premises infrastructure.

6. Availability and Transfer of Data

The Successful Bidder shall not withhold, restrict, delay, alter or otherwise obstruct the release or transfer of Bank Data, configurations, security content or other Bank-specific assets due to commercial, contractual or technical reasons.

Such data and information shall be made available to the Bank on demand during the contract period and in full during the transition phase.

7. Cloud-to-Cloud and Cloud-to-On-Premises Transition

Upon termination or expiry of the Agreement, or transition to another service provider or cloud environment, the Successful Bidder shall facilitate the complete and secure transfer of Bank Data and required configurations from the existing cloud environment to another CSP or the Bank's on-premises environment, as directed by the Bank.

The Successful Bidder shall provide the necessary technical assistance, coordination, configuration support, data extraction, data transfer, validation, reconciliation and documentation.

Raw and normalized logs shall be provided along with relevant metadata and information required for interpretation, investigation and threat hunting.

8. Exit and Transition Support

The Successful Bidder shall ensure seamless transfer of all Bank Data, configurations, security content, documentation and other required assets within a mutually agreed period of 60 to 90 days, extendable at the Bank's discretion by up to 30 additional days.

The transition shall be completed without data loss, corruption or avoidable service disruption and without any additional cost to the Bank.

9. Knowledge Transfer and Documentation

The Successful Bidder shall provide complete knowledge transfer and documentation necessary for continued operation of the Services, including:

a. Solution architecture and data-flow diagrams.
b. Configurations and integration details.
c. Log-source and data-source inventory.
d. SIEM use-case and correlation-rule catalogue.
e. SOAR playbooks and automation workflows.
f. Security monitoring and threat-hunting procedures.
g. SOPs, operational manuals and runbooks.
h. Incident handling and escalation procedures.
i. Known issues, exceptions, risks and pending activities.
j. Relevant tuning history and other operational information required for continued operation of the Services.

10. Credentials, Integrations and Endpoint Handover

The Successful Bidder shall provide or securely transfer all Bank-specific access configurations, certificates, API configurations, service account information, integration details and other technical information required for transition of the Services.

Where the Services involve endpoint agents, XDR agents, log forwarders, collectors or network sensors deployed across the Bank's infrastructure, the Successful Bidder shall provide all applicable agent tamper-protection credentials, maintenance tokens, uninstall keys and required decommissioning procedures, scripts or packages.

The Successful Bidder shall provide necessary assistance for their secure and phased removal or transition to the Replacement Bidder.

All credentials, certificates, keys and other sensitive information shall be transferred through secure mechanisms approved by the Bank.

Upon completion of the transition, all access provided to the Successful Bidder and its personnel shall be revoked, as applicable.

11. Data Integrity and Transition Validation

The Successful Bidder shall ensure that all data and security information transferred during the transition is complete, accurate and maintains its integrity.

The Bank or its authorized auditor may verify the completeness and integrity of:

a) Bank Data and raw/normalized logs.

b) Security configurations and security content.

c) Alerts, incidents, cases and investigation history.

d) Critical integrations and interfaces.

e) Documentation and knowledge transfer.

f) Data deletion and cryptographic erasure.

The Successful Bidder shall provide all reasonable assistance, evidence and information required for such verification.

12. Data Deletion and Cryptographic Erasure

Following successful migration and formal acceptance of the transition by the Bank, the Successful Bidder shall ensure complete and certified deletion of all Bank Data from all systems under its control, including production systems, test environments, temporary storage, backups, replicas, snapshots, disaster recovery and archival environments, subject to applicable legal and regulatory retention requirements.

Where Customer-Managed Keys (CMEK and/or BYOK) are utilized, the Successful Bidder shall, upon the Bank's written clearance, securely revoke and destroy the applicable encryption keys/key material in the Bank's/CSP's KMS/HSM in accordance with the approved key-management process, such that Bank Data encrypted using such keys can no longer be decrypted or accessed by the Successful Bidder, its subcontractors, cloud service providers or any other unauthorized third party.

The Successful Bidder shall ensure that cryptographic erasure covers all applicable copies of Bank Data protected by the relevant Customer-Managed Keys.

The Successful Bidder shall provide:

a) Immutable KMS/HSM key-destruction audit logs.

b) Applicable CSP storage-sanitization or deletion evidence.

c) Applicable CSP security or sanitization attestations/reports, where available.

d) A Cryptographic Erasure Certificate/Data Destruction Certificate duly signed by an authorized official confirming completion of the required activities.

13. Audit and Exit Acceptance

The Bank may appoint auditors to review and verify data transfer, security-content transfer, transition activities and cryptographic erasure/deletion.

Exit shall be considered complete only after formal acceptance by the Bank confirming satisfactory completion of the applicable transition activities, including:

a) Data transfer.

b) Security-content transfer.

c) Knowledge transfer.

d) Access and credential handover.

e) Data deletion and cryptographic erasure.

Release of the Successful Bidder's Performance Bank Guarantee (PBG) and final milestone/service payment shall remain contingent upon the Bank's issuance of formal Exit Acceptance sign-off.

14. Exit Testing

The Bank may, during the contract period, require the Successful Bidder to demonstrate the portability and exportability of Bank Data, configurations and security content through an exit or portability test.

The Successful Bidder shall provide reasonable assistance for such testing without adversely affecting the production Services.

15. Responsibility for Third Parties

The Successful Bidder shall remain fully responsible for ensuring that its subcontractors, cloud service providers, hosting providers and other third parties engaged in providing the Services comply with all applicable Exit Management requirements.

Failure by any subcontractor, cloud service provider, hosting provider or other third party shall not relieve the Successful Bidder of its obligations towards the Bank.

16. Compliance with Regulatory and Legal Requirements

All transition, data transfer, storage, processing, retention, cryptographic erasure and deletion activities shall comply with applicable Indian laws, regulations and regulatory directions, including those issued by RBI, SEBI, IRDAI, CERT-In and other applicable Government of India authorities.

The Successful Bidder shall comply with applicable requirements relating to data residency, data localization, information security, audit, record retention and preservation.

17. Exit Cost and Post-Exit Obligations

a) All activities necessary for Exit Management and Transition, including data extraction, export, migration support, configuration transfer, security-content transfer, documentation, knowledge transfer and technical assistance, shall be included in the Contract price and shall not attract any additional charges to the Bank.

b) Confidentiality, information security, protection of Bank Data, regulatory obligations and incident-related cooperation shall continue after termination or expiry of the Agreement to the extent applicable under the Agreement and applicable laws and regulations.

18. Regulatory Direction / Security Requirement

If the Successful Bidder fails to meet the guidelines, standards or requirements prescribed by the Government of India, RBI or any other applicable regulatory body within the timeframe specified by the Bank, or where the Bank is required to transition the Services pursuant to a regulatory or security requirement, the Bank reserves the right to terminate the Agreement and/or transition the Services to a different vendor without any additional exit or transition cost to the Bank.

In such circumstances, the Exit Management provisions shall apply in full.

15 APPENDIX

15.1 APPENDIX 1A: Functional Compliance Sheet (Solutions)

- Attached as a separate Excel file. Exceptions, disclaimers, limitations, conditional compliance submitted by bidder and / or OEMs in the bid shall not be taken on record and selected bidder & respective OEM must mandatorily provide such features, modules, add-ons, service etc. sought by the bank in the RFP.
- Generic, speculative & theoretical points should be avoided in the responses.

15.2 APPENDIX 1B: Technical Compliance Sheet (IT Infrastructure)

- Attached as a separate Excel file. Exceptions, disclaimers, limitations, conditional compliance submitted by bidder and / or OEMs in the bid shall not be taken on record and selected bidder & respective OEM must mandatorily provide such features, modules, add-ons, service etc. sought by the bank in the RFP.

- Generic, speculative & theoretical points should be avoided in the responses.

15.3 APPENDIX 1C: Functional Compliance Sheet (Services)

- Attached as a separate Excel file. Exceptions, disclaimers, limitations, conditional compliance submitted by bidder and / or OEMs in the bid shall not be taken on record and selected bidder & respective OEM must mandatorily provide such features, modules, add-ons, service etc. sought by the bank in the RFP.
- Generic, speculative & theoretical points should be avoided in the responses.

15.4 APPENDIX 2: Commercial Bill of material Sheet

Attached as a separate Excel file.

- Exceptions, disclaimers, limitations, conditional compliance submitted by bidder and / or OEMs in the bid shall not be taken on record and selected bidder & respective OEM must mandatorily provide such features, modules, add-ons, service etc. sought by the bank in the RFP.
- Generic, speculative & theoretical points should be avoided in the responses and shall be considered null and void

15.5 APPENDIX 3: IT Infrastructure Virtual To Physical (V2P) Mapping

Attached as a separate Excel file.

- Exceptions, disclaimers, limitations, conditional compliance submitted by bidder and / or OEMs in the bid shall not be taken on record and selected bidder & respective OEM must mandatorily provide such features, modules, add-ons, service etc. sought by the bank in the RFP.
- Generic, speculative & theoretical points should be avoided in the responses and shall be considered null and void

16 ANNEXURES

16.1 Annexure 1: Submission Checklist (on bidder's letterhead)

Sno	Particulars/ Document	To be submitted by on their letterhead	Submitted (yes/ no)	Page no.
1.	Annexure 1 – Submission checklist	Bidder		
2.	Annexure 2 – Bidder's Information	Bidder		
3.	Annexure 3 – Tender Covering Letter	Bidder		
4.	Annexure 4 – Bid Security Declaration	Bidder		
5.	Annexure 5 – Pre-Qualification Criteria	Bidder		
6.	Annexure 6 – Acceptance / Compliance Certificate	Bidder		
7.	Annexure 7 – Minimum Local Content, only if Applicable	Respective Solution / Service OEM		
8.	Annexure 8 – Certification on OEM Requirement	Respective Solution / Service OEM		
9.	Annexure 9A – Escalation Matrix	Bidder		
10.	Annexure 9B – Escalation Matrix	Respective Solution / Service OEM		
11.	Annexure 10 – Litigation Certificate	Bidder		
12.	Annexure 11 – Non-Blacklisting Undertaking	Bidder		
13.	Annexure 12 – Undertaking of Authenticity	Bidder		
14.	Annexure 13 – Non-Disclosure Agreement	Bidder		
15.	Annexure 15 – Bank Guarantee Format for EMD	Bidder		
16.	Annexure 17 – Pre-Contract Integrity Pact	Bidder		
17.	Annexure 18 – Compliance with FRS, TRS, SoW & SBOM	Respective Solution / Service OEM		
18.	Annexure 19 – Stack Confirmation Sheet	Bidder		

Sno	Particulars/ Document	To be submitted by on their letterhead	Submitted (yes/ no)	Page no.
19.	Annexure 20 – S-BOM & C-BOM Details of all Proposed Tools / Solutions	Respective Solution / Service OEM		
20.	Annexure 22A – Bidder Self-Declaration for Implementation Experience	Bidder mapped to the respective client and clause of PQ & TQ		
21.	Annexure 22B – OEM Self-Declaration for Implementation Experience	Respective Solution / Service OEM mapped to the respective client and clause of PQ & TQ		
22.	16.27 Annexure 26: Undertaking – Support & Launch Confirmation (on OEM's letterhead)	Respective IT infrastructure OEM of Compute, Storage (Primary, Long Term and Backup Storage/Appliance), Backup Solution and SAN Switch		
23.	Annexure 27 – Declaration regarding Prior Association with the Bank and Pending SLA/Contract	Bidder		
24.	Annexure 28 – Ownership Declaration and Contractual Performance	Bidder		
25.	Annexure 29 – Self-Declaration regarding Contract Cancellation / Termination / Rescission / Revocation	Bidder		
26.	Annexure 30 – Self-Declaration regarding Compliance with Applicable Labour Laws	Bidder		
27.	Annexure 31 – Declaration regarding Conflict of Interest and IT Security Vendor Restriction	Bidder		

Sno	Particulars/ Document	To be submitted by on their letterhead	Submitted (yes/ no)	Page no.
28.	Annexure 32 – OEM Functional Compliance Declaration	Respective Solution / Service OEM		
29.	Annexure 33 – Back-to-back support/ backlining confirmation	Respective Solution / Service OEM		
30.	Annexure 35 – OEM Compliance & Action Taken Report	Respective Solution / Service OEM		
31.	Technical Presentation along with OEM Proposed Project Timelines, Milestones, Tasks & Sub-Tasks	Bidder		
32.	Signed Copy of RFP along with Corrigenda / Addenda, if any	Bidder		
33.	Appendix 1A – Functional Compliance (Solutions)	Respective Solution / Service OEM		
34.	Appendix 1B – Technical Compliance	Respective Hardware & Backup OEM		
35.	Appendix 1C – Functional Compliance (Services)	Respective Security Service OEM		
36.	Appendix 3 – IT Infrastructure v2P	Bidder		
37.	Masked Appendix 2 – Bill of Material with all required details	Bidder		
38.	OEM Product Datasheets / Technical Manuals / Supporting Documents	Respective Solution / Service OEM and Hardware OEMs		
39.	Supporting documents for implementation experience / client references	Bidder / OEM, as applicable		

Filling Notes: **Masked Bill of Material**

1. Masked **BoM is a mandatory part of the Technical Proposal**. It must provide the Bank with complete visibility of the proposed solution components **without revealing any commercial/pricing information**. The Masked BoM shall contain **no commercial, financial, pricing, or other price-related information whatsoever**.

2. The Masked BoM shall cover **all products, licenses, hardware, software, subscriptions, services, implementation components, support services, and all other components** proposed by the Bidder as part of the solution.
3. The Masked BoM shall be an **exact replica of the Commercial BoM** with respect to all non-commercial particulars, including but not limited to:
    a. Item description;
    b. Product/solution name;
    c. OEM/Manufacturer name;
    d. Model number;
    e. Part number/SKU;
    f. Technical specifications;
    g. Quantity;
    h. Unit of measurement;
    i. License/subscription details; and
    j. Other solution/component details.
4. The Bidder shall ensure that the **item descriptions, quantities, specifications, part numbers and solution components in the Masked BoM exactly correspond to those provided in the Commercial BoM**. No item shall be added, deleted, substituted, or modified in a manner that results in inconsistency between the two BoMs
5. The Bidder shall be solely responsible for ensuring that the Masked BoM does not disclose any commercial or pricing information in the Technical Proposal.
6. Failure to submit the Masked BoM, submission of an incomplete Masked BoM, or submission of a Masked BoM containing any commercial/pricing information shall constitute non-compliance with the RFP and may render the Bidder's Technical Proposal liable for rejection, at the sole discretion of the Bank.
7. The Masked BoM shall include complete technical and quantity details of the proposed solution, such as **Solution-Solution/Product, Model, Version, Edition, Licensing Metric, Quantity, OEM/Manufacturer, Part Number and Technical Specifications**. **Services** – OEM, solution name, scope, modules, subscription/monitoring coverage and quantity; **Servers** – OEM, model, processor, memory, storage, network configuration and quantity; **Storage** – OEM, model, usable capacity, controller and connectivity details;
8. **Backup Solution** – OEM, software, licenses, backup capacity, retention and supported workloads; and other proposed products/services.
9. All commercial information, including **unit cost, total cost, taxes, GST, discounts, duties and any other commercial value, shall be masked as "XX"**.

Note:
All pages of the bid documents must be sealed & signed in full by authorized person.
All pages of the bid documents should be numbered in serial order i.e. 1, 2, 3….
Bank may ask for any other document on its discretion.
All declarations/undertakings should be: a) **on the required letterhead, wherever prescribed;** b) **signed by the authorized signatory;** c) **stamped/sealed wherever required;** d) **dated;** e) **supported by documentary evidence wherever the RFP asks for evidence**
OEM documents should be obtained from the respective Security Solution/Service OEM
Wherever an OEM document is required, ensure the OEM name and the corresponding proposed product/service in the technical proposal are clearly identifiable.

Signature & Seal of the Bidder

16.2 Annexure 2: Bidder's Information

Bidder's Information

(Should be submitted on Company's letter head with company seal and signature of the authorized person)

Reg: Request for proposal for Selection of bidder for supply installation, implementation, maintenance & management of NextGen SOC & related services

Ref: RFP No._____ dated_____

#	Particulars	Details
1.	Name of the Company Address for Correspondence: Registered Office: Corporate Office:	
2.	Constitution (Proprietary/Partnership/Private Ltd./Public Ltd./ LLP/ Others)	
3.	Registration No. and date of establishment	
4.	Website Address	
5.	Email Address	
6.	Number of Years in the Business	
7.	Detail of Earnest Money Deposited.	
8.	If any exemption is required with respect to EMD or Start-up.	
9.	Income Tax PAN GSTN ID Beneficiary Bank Details Beneficiary Name Beneficiary Account Number Type of Account (OD/OCC etc.) IFSC Name of the Bank and Branch address	
10.	Single Point of contact for this RFP Name: Designation: Mobile No.: Landline No.: Email-ID (any changes in the above should be informed in advance to Bank)	
11.	Name of Person Authorized to sign Designation.	

	Mobile No. Email Address	

Wherever applicable submit documentary evidence to facilitate verification.

DECLARATION:

I/We hereby declare that the terms and conditions of the tender stated herein and as may be modified/mutually agreed upon are acceptable and binding to me/us. We understand and agree and undertake that: -

1. The Bank is not bound to accept the lowest bid or may reject all or any bid at any stage at its sole discretion without assigning any reason, therefore.
2. If our Bid for the above job is accepted, we undertake to enter into and execute at our cost, when called upon by the Bank to do so, a contract in the prescribed form. Unless and until a formal contract is prepared and executed, this bid together with your written acceptance thereof shall constitute a binding contract between us.
3. We have read and understood all the terms and conditions and contents of the RFP and also undertake that our bid conforms to all the terms and conditions and does not contain any deviation and misrepresentation. We understand that the bank reserves the right to reject our bid on account of any misrepresentation/deviations contained in the bid.
4. Bank may accept or entrust the entire work to one Bidder or divide the work to more than one bidder without assigning any reason or giving any explanation whatsoever and the Bank's decision in this regard shall be final and binding on us.
5. I/ We do not have any conflict of interest as mentioned in the RFP document.
6. I/We submit this application under and in accordance with the terms of the RFP document and agree and undertake to abide by all the terms and conditions of the RFP document.
7. The Prices submitted by us have been arrived at without agreement with any other Bidder of this RFP for the purpose of restricting competition.
8. The prices submitted by us have not been disclosed and will not be disclosed to any other Bidder responding to this RFP.
9. We have not induced or attempted to induce any other Bidder to submit or not to submit a Bid for restricting competition.
10. We have quoted for all the services/items mentioned in this RFP in our price Bid.
11. The rate quoted in the price Bids are as per the RFP and subsequent pre-Bid clarifications/ modifications/ revisions furnished by the Bank, without any exception.
12. We agree to the splitting of order in the proportion as stated in the RFP at the discretion of Bank.
13. We certify that while submitting our Bid document, we have not made any changes in the contents of the RFP document, read with its amendments/clarifications provided by the Bank.
14. If our bid is accepted, we are to be jointly and severally responsible for the due performance of the contract.
15. We ensured that salary payments to resources deployed for Bank's Project is done through Transfer mode from bidder's Bank a/c directly to credit into their specific salary accounts only.

No cash payments are to be made to provide remuneration for services provided to the Bank on behalf of the selected bidder.

16. Bidder means the vendor(s) who is decided and declared so after examination of commercial bids.
17. We ensure that the entire data relating to payment systems operated by them will be stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction.
18. We confirm that Payment of statutory dues like PF, ESIC etc. are being made on time to the employees.

Date:

Place:

Bidder's Authorized Signatory

Designation

Bidder's name

Company Name and Seal

16.3 Annexure 3: Tender Covering Letter

Tender Covering Letter

(Should be submitted on Company's letter head)

To General Manager (CISO)

STAFF TRAINING CENTRE PUNJAB AND SIND BANK

Punjab & Sind Bank, CISO cell 3rd Floor,

B-8/232, Naharpur Village Rd, Pocket 8, Sector 3B,

Rohini, Delhi, 110085

Dear Sir,

Sub: Request for proposal for Selection of bidder for supply installation, implementation, maintenance & management of NextGen SOC & related services

Ref No._____ dated _____

We hereby confirm and undertake that:

1. Authorization: The undersigned is duly authorized to sign and submit the Bid and all related documents on behalf of [Bidder Name]. A copy of the applicable Authorization Letter / Power of Attorney / Board Resolution is enclosed with the Bid.
2. Acceptance of Terms and Conditions: We unconditionally agree to abide by and fulfil all the terms, conditions, requirements and obligations stipulated in the RFP. In the event of any default, we shall be liable for the consequences, including forfeiture or payment of such amounts as may be applicable under the RFP and/or resultant contract.
3. No Deviation: We confirm that our Bid has been submitted in accordance with the requirements of the RFP and that there are no assumptions, reservations, conditions, deviations, exclusions, extraneous conditions, or qualifications from the prescribed terms and conditions, except those expressly permitted and accepted by the Bank. We understand that any no assumptions, reservations, conditions, deviations, exclusions, extraneous conditions, or qualifications or non-compliance may result in rejection/disqualification of our Bid, as per the provisions of the RFP. Any such matter shall be deemed **withdrawn, null and void and non-binding on the Bank**, and we shall remain fully responsible for complying with the corresponding RFP requirement.
4. Binding Offer: We hereby unconditionally and irrevocably accept all the terms, conditions, requirements, obligations and provisions contained in the RFP and undertake to comply with the same throughout the procurement and contractual period.

5. We agree that the RFP, our Bid, the Bank's written acceptance/Notification of Award (NoA)/Letter of Intent (LOI), and the resultant Contract and SLAs shall govern our obligations in accordance with the provisions of the RFP..
6. Bank's Right to Accept/Reject: We understand and acknowledge that the Bank is not bound to accept the lowest or any Bid and may accept or reject any Bid in accordance with the provisions of the RFP.
7. Non-Blacklisting: We certify that, [Bidder/SI Name] has not been blacklisted, debarred, suspended or declared ineligible by any Regulator, Statutory Body, Central/State Government, Government Agency, Bank or Financial Institution in India during the last three (3) years preceding the date of Bid submission and as on the date of Bid submission
8. Accuracy of Information: We certify that all information, statements, documents and claims submitted by us in connection with the Bid are true, complete and correct to the best of our knowledge and belief.
9. We undertake that all requirements necessary for fulfilment of our obligations under the RFP, including resources, products, services, licences, infrastructure, support and other deliverables expressly covered within the scope of the RFP, shall be provided at the prices quoted in our Commercial Bid and without any additional cost to the Bank.
10. Verification and Misrepresentation: We acknowledge that the Bank reserves the right to independently verify/evaluate any information, claim, credential or document submitted by us. In case of any misrepresentation, concealment or submission of false/inaccurate information at any stage of the selection or contract period, the Bank shall have the right to reject/disqualify our Bid and/or take such action as may be provided under the RFP and applicable contract.
11. We certify that all information, statements, documents, certificates, declarations and supporting evidence submitted by us in connection with this RFP are true, complete, accurate and authentic to the best of our knowledge and belief.
12. We undertake to execute and submit the duly signed Contract, NDA, SLA and other documents required under the RFP within the 15 days of PO Acceptance. Failure to execute or submit such documents within the stipulated period shall entitle the Bank to take action in accordance with the RFP, including forfeiture of EMD and/or cancellation of the Purchase Order/award, or any other as applicable.

We hereby confirm our full commitment to comply with the requirements of the RFP and all obligations arising therefrom.

Dated this ____day of _____, 2026

Authorized Signatory

Designation

Bidder’s name

(Name of Address Authorized Signatory)

Company Name and Seal

16.4 Annexure 4: Bid Security Declaration

Bid Security Declaration

(To be stamped in accordance with stamp act)

(Should be submitted by eligible MSEs/Startups on Company's letter head with company seal and signature of the authorized person)

Date: _____

To,

General Manager (CISO)

STAFF TRAINING CENTRE PUNJAB AND SIND BANK

Punjab & Sind Bank, CISO cell 3rd Floor,

B-8/232, Naharpur Village Rd, Pocket 8, Sector 3B,

Rohini, Delhi, 110085

Dear Sir,

We, the undersigned, declare that:

We, M/s…….. (herein referred to as bidder) understand that, according to bid clause No. 1.12, bids may be supported with a Bid Security Declaration, bidder render the declaration that:-

Bank may proceed against us for recovery of actual direct losses as per the remedy available under an applicable law (maximum up to Rs……../-) and In case of Execution of Bid Security Declaration, we, M/s……..may be suspend for three (3) years from being eligible to submit our bids for any contracts with the Bank if we, M/s…….. are in breach of our obligation(s) under the bid conditions, in case we, M/s……..:-

- Fails to honor submitted bid; and/or
- If the bidder withdraws the bid during the period of bid validity (180 days from the date of opening of bid).
- If the bidder makes any statement or encloses any form which turns out to be false, incorrect and / or misleading at any time prior to signing of contract and/or conceals or suppresses material information; and / or
- The selected bidder withdraws his tender before furnishing the unconditional and irrevocable Performance Bank Guarantee.
- The bidder violates any of the provisions of the terms and conditions of this tender specification.
- In case of the successful bidder, if the bidder fails:
  - To sign the contract in the form and manner to the satisfaction of Punjab & Sind Bank
  - To furnish Performance Bank Guarantee in the form and manner to the satisfaction of Punjab & Sind Bank either at the time of or before the execution of Agreement.

- Bank may proceed against the selected bidder in the event of any evasion, avoidance, refusal or delay on the part of bidder to sign and execute the Purchase Order / Service Level Agreements or any other documents, as may be required by the Bank, if the bid is accepted.

We, M/s……..understand that this declaration shall expire if we are not the successful bidder and on receipt of purchaser's notification of the award to another bidder; or forty-five days after the validity of the bid; whichever is later.

Name of Signatory

Designation

16.5 Annexure 5: Pre-Qualification Criteria

Ref: RFP No._____ dated_____Date: _____

#	Eligibility Criteria/Clause	Documents Required
1.	Proof of Earnest Money Deposit	To be submitted along with the bid.
2.	The Bidder should be operating in India as a registered company under Companies Act, 2013/1956 or LLP (Limited Liability Partnership) Act 2008 or Partnership firms registered under the Indian Partnership Act, 1932 with registered offices in India, and should be in existence in India for at least the last 5 (five) years as on date of opening of the bid	Copy of Certificate of Incorporation or Partnership Deed AND Copy of Registration Certificate/GST Registration certificate Copies of all documents listed above should be attested by authorized signatory and must be submitted along with the response.
3.	The bidder should have valid PAN and GST Registration in India	Copy of Valid PAN Card, GST Registration Certificates issued by competent authority in India
4.	The bidder should have a minimum average turnover of INR 500 crore per annum in India during the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth. Note – In case of MSMEs only, the turnover may be relaxed subject to meeting the quality and technical specifications.	CA Certificate mentioning the turnover and net worth for each financial year. and Audited Financial statements (Balance sheet & Profit & Loss statement). The CA certificate provided in this regard should be without any riders or qualification.
5.	The bidder should be an authorized representative/ partner/ reseller of OEM in India. MAF should be submitted from the following solution OEMs: 1. SIEM 2. SOAR 3. UEBA 4. Extended Detection & response (XDR) 5. Decoy/HoneyPot/Deception 6. Threat Intelligence Platform 7. Vulnerability Assessment & vulnerability Lifecycle Management	MAF from the respective OEMs of the solution & services containing- 1. Name and address of the OEM and the name and address of the authorised bidder/entity. 2. Confirmation that the bidder/entity is duly authorised by the OEM for supply, installation, implementation, technical support, maintenance and related services for the proposed solution(s). The MAF shall be submitted on the official letterhead of the respective OEM and must be signed by an authorised signatory having the authority to bind the OEM."

#	Eligibility Criteria/Clause	Documents Required
	8. Identity Threat Detection & response 9. Application Security Testing 10. Cloud Security Posture Management (CSPM) 11. Cloud-Native Application Protection Platform (CNAPP) 12. Cloud Workload Protection Platform (CWPP) 13. Continuous Threat Exposure Management (CTEM) MAF should also be submitted from the following services OEMs: 1. Breach Attack & Simulation 2. Continuous Automated Red Teaming services 3. Attack Surface management 4. Phishing simulation 5. Digital risk management 6. Dark web monitoring 7. Threat Intelligence feed 8. Threat hunting services	
6.	Bidder must have at least enrolled manpower (on bidder's payroll) of 100 experienced employees skilled in areas of Cyber security.	Self-certification from the bidder
7.	The bidder must have experience of having successfully installed and maintained (and currently maintaining) and/or managing the SIEM Solution, with a minimum capacity of 20,000 EPS / 0.86 TB per day, as stipulated in the RFP, for a single eligible client falling within the categories specified in the RFP, in India, during the last five years. The stipulated 20,000 EPS / 0.86 TB per day requirement shall be demonstrated for a single eligible client and a single SIEM deployment/environment.	Bidder to Submit the following 3 Documents: Document 1: Copy of Purchase Order / Work Order / Contract The submitted client-issued document shall clearly indicate, either directly or through a combination of documents forming part of the same contract: a. Name of the Client. b. Date of Issue/Signing. c. Scope of Work demonstrating installation and maintenance/AMC/support of the SIEM Solution. d. Solution Name and OEM Name

#	Eligibility Criteria/Clause	Documents Required
	Note: - A Bidder's experience shall be considered irrespective of when the implementation was completed. Even if the implementation was completed more than five years prior to the date of publication of the RFP, such experience shall qualify only where the same Bidder that supplied, installed and implemented the SIEM Solution is also currently maintaining the same solution, or has maintained the same solution at any time during the five-year period preceding the date of publication of the RFP. The aggregate EPS/log volume of multiple tenants, clients, subsidiaries, sites, SIEM instances or separate deployments shall not be considered for meeting the stipulated threshold.	e. SIEM Sizing/Capacity implemented, clearly indicating minimum 20,000 EPS or 0.86 TB/day AND Document 2: Client-Issued Supporting Document (Any-One) Any one of the following client-issued documents: a. Client Credential/Experience Certificate; or b. Email Confirmation from the Client clearly stating the PO Number.; or c. Client-signed Installation/Implementation Report; or d. Client Acceptance/Go-Live/Completion/Sign-off Certificate; or e. Extension Letter The client-issued supporting document shall clearly establish, as applicable: • Name of the Client. • Project/Solution Name. • Successful - Installation and Commissioning/Implementation of the SIEM Solution. • Maintenance/Support/AMC status (completed or under maintenance). • SIEM Capacity implemented (EPS and/or TB/day) • Date(s) establishing that the project falls within the required eligibility period. AND

#	Eligibility Criteria/Clause	Documents Required
		Document 3: Bidder's Self-Declaration (in the format Annexure 22A) The Bidder shall submit a Self-Declaration cross-referencing the submitted documentary evidence and providing the following details: a. Project Name. b. Client Name. c. Client Category (PSU/ PSE/ Government Organizations / BFSI/Telecom). d. Scope Executed: e. Installation – Yes/No f. Maintenance / Under Maintenance – Yes/No g. Contract Period: 1. Start Date 2. End Date h. Solution Name. i. OEM Name. j. Implemented SIEM Capacity (EPS and/or TB/day). k. Reference to the submitted client-issued document(s), including: 3. Document Name. 4. Relevant Page Number(s). 5. Clause/Section/Page where the following are evidenced: i. Client Name. ii. Scope of Work. iii. Solution Name. iv. SIEM Capacity (EPS/TB/day). v. Maintenance/Support Status. vi. Contract/Project Period.

#	Eligibility Criteria/Clause	Documents Required
8.	Bidder should have supplied, installed and maintained (or under maintenance) any three (3) of the below solutions in any one PSU/PSE/ Government Organizations / BFSI/Telecom provider in India a. SOAR b. UEBA c. Extended Detection & response (XDR)/ Endpoint Detection & response (EDR)/ Network Detection & response (NDR)/Network Behaviour Anomaly Detection (NBAD) d. Threat Intelligence Platform e. Vulnerability Assessment/Vulnerability management f. Identity Threat Detection & response g. Decoy/Honeypot/Deception h. Application security testing tool (DAST or SAST) i. Cloud Security Posture Management (CSPM) j. Cloud-Native Application Protection Platform (CNAPP) k. Cloud Workload Protection Platform (CWPP) l. Continuous Threat Exposure Management (CTEM) Note: - Experience of solutions can be shown in single /multiple Clients/ work orders meeting the above criteria experience in installing a solution will be considered regardless of when the installation was completed. Even if the installation was completed more than five years ago, it will still qualify, provided that the same bidder is currently maintaining that solution or has carried out its maintenance at any time during the five-year period preceding the RFP publication date	Bidder to Submit the following 3 Documents: Document 1: Copy of Purchase Order / Work Order / Contract The submitted client-issued document shall clearly indicate, either directly or through a combination of documents forming part of the same contract: a. Name of the Client. b. Date of Issue/Signing. c. Scope of Work demonstrating installation and maintenance/AMC/support of the respective Solution. d. Solution Name and OEM Name AND Document 2: Client-Issued Supporting Document (Any-One) Any one of the following client-issued documents: a. Client Credential/Experience Certificate; or b. Email Confirmation from the Client; or c. Client-signed Installation/Implementation Report; or d. Client Acceptance/Go-Live/Completion/Sign-off Certificate; or e. Extension Letter The client-issued supporting document shall clearly establish, as applicable: • Name of the Client. • Project/Solution Name. • Successful Installation and Commissioning/Implementation.

#	Eligibility Criteria/Clause	Documents Required
		• Maintenance/Support/AMC status (completed or under maintenance). • Date(s) establishing that the project falls within the required eligibility period. Note: If all the above information is not available in a single client-issued document, the Bidder may submit a combination of client-issued documents, provided that together they establish compliance with the eligibility criteria. AND Document 3: Bidder's Self-Declaration (in the format Annexure 22A) The Bidder shall submit a Self-Declaration cross-referencing the submitted documentary evidence and providing the following details: a. Project Name. b. Client Name. c. Client Category (PSU/PSE/ Government Organizations / BFSI/Telecom) d. Scope Executed: e. Installation – Yes/No f. Maintenance / Under Maintenance – Yes/No g. Contract Period: a. Start Date b. End Date h. Solution Name. i. OEM Name. j. Reference to the submitted client-issued document(s), including: a. Document Name. b. Relevant Page Number(s).

#	Eligibility Criteria/Clause	Documents Required
		c. Clause/Section/Page where the following are evidenced: i. Client Name. ii. Scope of Work. iii. Solution Name. iv. Maintenance/Support Status. v. Contract/Project Period.
9.	Bidder must have back-to-back support relation with the proposed OEMs of solutions & services.	Self-Declaration from the bidder's authorized signatory as per the format Annexure 33: Confirmation for Backlining
10.	If the bidder or its subsidiary or its associate or sister company or its holding company has already had an association with Punjab & Sind Bank in the past 5 years or at present as a service provider on any project, then the bidder is required to submit the satisfactory certificate from the bank issued/dated post the issuance of the RFP. Additionally, the Bidder should not have any Service Level Agreement/Contract pending to be signed with the Bank pending for more than 6 months from the date of issue of purchase order	Self-Certification from the bidder in the format Annexure 27: Association with Bank
11.	The Bidder to provide information that none of its subsidiaries or sister company or associate or holding company or companies having common director/s or companies in the same group of promoters/management or partnership firms/LLPs having common partners is not owned by any Director or Employee of the Bank.	Self-Certification from the bidder (in the format Annexure 28: Ownership Declaration and Contractual performance)
12.	The bidder shall submit a self-declaration confirming that, during the last three (3) years preceding the date of publication of this RFP, no contract, Purchase Order, or award issued by Punjab & Sind Bank (PSB) to the bidder has been cancelled, terminated, rescinded, or revoked due to non-performance,	Self-Certification from the bidder (in the format Annexure 29: Contract Cancellation / Termination / Rescission / Revocation)

#	Eligibility Criteria/Clause	Documents Required
	breach of obligations, or failure to comply with post-award requirements.	
13.	The Bidder should not have been blacklisted/ debarred by the Regulator / statutory body/ Government / Government agency / Banks / Financial Institutions in India during last 3 years and as on the date of bid submission.	Self-Certification from the bidder as per Annexure 11
14.	The bidder should not be involved in any litigation which threatens the solvency of company.	Self-Certification from the bidder as per Annexure 10
15.	Labor Law Compliance	Self-Certification from the bidder as per the format provided in Annexure 30
16.	Integrity Pact	Document on 100 Rs Stamp paper, duly signed and stamped by the authorized signatory. (As per Annexure 17)
17.	Non-Disclosure Agreement	Document on 100 Rs Stamp paper, duly signed and stamped by the authorized signatory. (As per Annexure 13)
18.	To ensure conflict of interest the successful bidder or its subsidiary or its associate or sister company or its holding company should not be the **IT Security or NOC vendor** of the bank under the existing or new contract.	Self-declaration signed by Authorized Signatory of the bidder (as per Annexure 31)
OEM Evaluation Criteria		
19.	The proposed OEM SIEM Solution with a minimum capacity of 30,000 EPS or 1.2 TB/day shall have been successfully implemented and be under management/maintenance in at least one (1) BFSI client in India. The stated minimum capacity of 30,000 EPS or 1.2 TB/day shall be demonstrated in the referenced client only and shall not be aggregated or combined across multiple clients/references. **and** The proposed OEM SIEM Solution with a minimum capacity of 30,000 EPS or 1.2 TB/day shall have been successfully	Document 1: Copy of Purchase Order / Work Order / Contract The submitted client-issued document shall clearly indicate, either directly or through a combination of documents forming part of the same contract: a. Name of the Client. b. Date of Issue/Signing. c. Scope of Work. d. Solution Name and OEM Name e. SIEM Capacity, clearly indicating one of the following, as applicable: a. Minimum 30,000 EPS or 1.2 TB/day. b. On-premises/Cloud Deployment

#	Eligibility Criteria/Clause	Documents Required
	implemented on cloud in atleast one (1) client in India. The stated minimum capacity of 30,000 EPS or 1.2 TB/day shall be demonstrated in the referenced client only and shall not be aggregated or combined across multiple clients/references. Note: - experience in installing a solution will be considered regardless of when the installation is completed. Even if the installation was completed more than five years ago, it will still qualify, provided that the same bidder is currently maintaining that solution or has carried out its maintenance at any time during the five-year period preceding the RFP publication date. The aggregate EPS/log volume of multiple tenants, clients, subsidiaries, sites, SIEM instances or separate deployments shall not be considered for meeting the stipulated threshold.	OR Document 2: Client-Issued Supporting Document (Any-One) Any one of the following client-issued documents: a. Client Credential/Experience Certificate; or b. Email Confirmation from the Client; or c. Client-signed Installation/Implementation Report; or d. Client Acceptance/Go-Live/Completion/Sign-off Certificate; or e. AMC/Support Confirmation/Extension Letter or f. Client-issued Project Status/Progress Certificate (for projects under implementation) The client-issued supporting document shall clearly establish, as applicable: • Name of the Client. • Project/Solution Name. • Project Status, clearly indicating one of the following ○ Implemented & Managed; ○ Under Maintenance/Managed Services; ○ Under Implementation. • SIEM Capacity implemented/under implementation (EPS and/or TB/day) • Date(s) establishing that the project falls within the required eligibility period.

#	Eligibility Criteria/Clause	Documents Required
		Note: If all the above information is not available in a single client-issued document, the Bidder may submit a combination of client-issued documents, provided that together they establish compliance with the eligibility criteria. AND Document 3: OEM's Self-Declaration (as per **Annexure 22B: OEM Self-Declaration for Implementation Experience)** The OEM shall submit a Self-Declaration cross-referencing the submitted documentary evidence and providing the following details: a. Project Name. b. Client Name. c. Client Category (BFSI). d. Contract Period: a. Start Date b. End Date e. Solution Name. f. Project Status (Select one): a. Implemented & Managed; b. Under Maintenance; c. Under Implementation. g. SIEM Capacity (EPS and/or TB/day). h. Reference to the submitted client-issued document(s), including: a. Document Name. b. Relevant Page Number(s). c. Clause/Section/Page where the following are evidenced: i Client Name. ii Scope of Work.

#	Eligibility Criteria/Clause	Documents Required
		iii Solution Name. iv SIEM Capacity (EPS/TB/day). v Maintenance/Support Status. vi Contract/Project Period. vii Project Status (Implemented & Managed / Under Maintenance / Under Implementation)
20.	The proposed OEM solution should have been implemented in at least one BFSI client is to be submitted for the following solutions: 1. SOAR 2. UEBA 3. Extended Detection & response (XDR) 4. Threat Intelligence Platform Note: - Experience of solutions can be shown in single /multiple Clients/ work orders meeting the above criteria A bidder's experience in installing a solution will be considered regardless of when the installation was completed. Even if the installation was completed more than five years ago, it will still qualify, provided that the same bidder is currently maintaining that solution or has carried out its maintenance at any time during the five-year period preceding the RFP publication date	Document 1: Copy of Purchase Order / Work Order / Contract The submitted client-issued document shall clearly indicate, either directly or through a combination of documents forming part of the same contract: a. Name of the Client. b. Date of Issue/Signing. c. Scope of Work demonstrating - installation and maintenance/AMC/support of the respective Solution. d. Solution Name and OEM Name OR Document 2: Client-Issued Supporting Document (Any-One) Any one of the following client-issued documents: a. Client Credential/Experience Certificate; or b. Email Confirmation from the Client; or c. Client-signed Installation/Implementation Report; or d. Client Acceptance/Go-Live/Completion/Sign-off Certificate; or e. AMC/Support Confirmation/Extension Letter

#	Eligibility Criteria/Clause	Documents Required
		The client-issued supporting document shall clearly establish, as applicable: • Name of the Client. • Project/Solution Name. • Successful Installation and Commissioning/Implementation. • Maintenance/Support/AMC status (completed or under maintenance). • Date(s) establishing that the project falls within the required eligibility period. Note: If all the above information is not available in a single client-issued document, the Bidder may submit a combination of client-issued documents, provided that together they establish compliance with the eligibility criteria. AND Document 3: OEM's Self-Declaration (as per **Annexure 22B: OEM Self-Declaration For Implementation Experience)** The OEM shall submit a Self-Declaration cross-referencing the submitted documentary evidence and providing the following details: 1. Project Name. 2. Client Name. 3. Client Category (BFSI) 4. Scope Executed: 5. Installation – Yes/No 6. Maintenance / Under Maintenance – Yes/No 7. Contract Period: a. Start Date b. End Date 8. Solution Name.

#	Eligibility Criteria/Clause	Documents Required
		9. OEM Name. 10. Reference to the submitted client-issued document(s), including: a. Document Name. b. Relevant Page Number(s). c. Clause/Section/Page where the following are evidenced: vi. Client Name. vii. Scope of Work. viii. Solution Name. ix. Maintenance/Support Status. x. Contract/Project Period.
21.	The proposed OEM solution should have been implemented in at least one Scheduled Commercial Bank/PSU/ PSE/Government Organizations / BFSI/ in India. Credential is to be submitted for the following solutions: 1. Decoy/Honey-Pot/Deception 2. Vulnerability Assessment/Vulnerability management 3. Identity threat detection and response (ITDR) 4. Application Security testing Tool (SAST & DAST) 5. Cloud Security solution (CSPM) Note: - Experience of solutions can be shown in single /multiple Clients/ work orders meeting the above criteria A bidder's experience in supplying and installing a solution will be considered regardless of when the installation was completed. Even if the installation was completed more than five years ago, it will still qualify, provided the bidder is currently maintaining that solution or has carried out its	Document 1: Copy of Purchase Order / Work Order / Contract The submitted client-issued document shall clearly indicate, either directly or through a combination of documents forming part of the same contract: a. Name of the Client. b. Date of Issue/Signing. c. Scope of Work demonstrating supply, installation and maintenance/AMC/support of the respective Solution. d. Solution Name and OEM Name OR Document 2: Client-Issued Supporting Document (Any-One) Any one of the following client-issued documents: a. Client Credential/Experience Certificate; or b. Email Confirmation from the Client; or c. Client-signed Installation/Implementation Report; or

#	Eligibility Criteria/Clause	Documents Required
	maintenance at any time during the five-year period preceding the RFP publication date	d. Client Acceptance/Go-Live/Completion/Sign-off Certificate; or e. AMC/Support Confirmation/Extension Letter The client-issued supporting document shall clearly establish, as applicable: • Name of the Client. • Project/Solution Name. • Successful Supply, Installation and Commissioning/Implementation. • Maintenance/Support/AMC status (completed or under maintenance). • Date(s) establishing that the project falls within the required eligibility period. Note: If all the above information is not available in a single client-issued document, the Bidder may submit a combination of client-issued documents, provided that together they establish compliance with the eligibility criteria. AND Document 3: OEM's Self-Declaration (as per **Annexure 22B: OEM Self-Declaration For Implementation Experience)** The OEM shall submit a Self-Declaration cross-referencing the submitted documentary evidence and providing the following details: 1. Project Name. 2. Client Name. 3. Client Category (Scheduled Commercial Bank/PSU/ PSE/Government Organizations / BFSI/) 4. Scope Executed:

#	Eligibility Criteria/Clause	Documents Required
		5. Installation – Yes/No 6. Maintenance / Under Maintenance – Yes/No 7. Contract Period: a. Start Date b. End Date 8. Solution Name. 9. OEM Name. 10. Reference to the submitted client-issued document(s), including: a. Document Name. b. Relevant Page Number(s). c. Clause/Section/Page where the following are evidenced: i. Client Name. ii. Scope of Work. iii. Solution Name. iv. Maintenance/Support Status. v. Contract/Project Period.
22.	The proposed OEM solution should have been implemented in at least one verifiable client in India. Credential is to be submitted for the following solutions: a. CNAPP b. CWPP c. CTEM Note: - Experience of solutions can be shown in single /multiple Clients/ work orders meeting the above criteria	Document 1: Copy of Purchase Order / Work Order / Contract The submitted client-issued document shall clearly indicate, either directly or through a combination of documents forming part of the same contract: a. Name of the Client. b. Date of Issue/Signing. c. Scope of Work demonstrating installation and maintenance/AMC/support of the respective Solution. d. Solution Name and OEM Name OR Document 2: Client-Issued Supporting Document (Any-One)

#	Eligibility Criteria/Clause	Documents Required
	experience in installing a solution will be considered regardless of when the installation was completed. Even if the installation was completed more than five years ago, it will still qualify, provided the bidder is currently maintaining that solution or has carried out its maintenance at any time during the five-year period preceding the RFP publication date	Any one of the following client-issued documents: a. Client Credential/Experience Certificate; or b. Email Confirmation from the Client; or c. Client-signed Installation/Implementation Report; or d. Client Acceptance/Go-Live/Completion/Sign-off Certificate; or e. AMC/Support Confirmation/Extension Letter The client-issued supporting document shall clearly establish, as applicable: • Name of the Client. • Project/Solution Name. • Successful Installation and Commissioning/Implementation. • Maintenance/Support/AMC status (completed or under maintenance). • Date(s) establishing that the project falls within the required eligibility period. Note: If all the above information is not available in a single client-issued document, the Bidder may submit a combination of client-issued documents, provided that together they establish compliance with the eligibility criteria. AND Document 3: OEM's Self-Declaration (as per **Annexure 22B: OEM Self-Declaration For Implementation Experience)**

#	Eligibility Criteria/Clause	Documents Required
		The OEM shall submit a Self-Declaration cross-referencing the submitted documentary evidence and providing the following details: a. Project Name. b. Client Name. c. Client Category (Scheduled Commercial Bank/PSU/ PSE/Government Organizations / BFSI/ Fortune 500 Companies (2024/2025/2026) d. Scope Executed: e. Installation – Yes/No f. Maintenance / Under Maintenance – Yes/No g. Contract Period: a. Start Date b. End Date h. Solution Name. i. OEM Name. j. Reference to the submitted client-issued document(s), including: a. Document Name. b. Relevant Page Number(s). c. Clause/Section/Page where the following are evidenced: i. Client Name. ii. Scope of Work. iii. Solution Name. iv. Maintenance/Support Status. v. Contract/Project Period.
23.	The proposed OEM services should have been implemented in at least one (1) PSU/ PSE/ Government Organizations / BFSI in India.	Document 1: Copy of Purchase Order / Work Order / Contract The submitted client-issued document shall clearly indicate, either directly or through a combination of documents forming part of the same contract:

#	Eligibility Criteria/Clause	Documents Required
	Credential is to be submitted for the following services: 1. Breach Attack & Simulation 2. Continuous Automated Red Teaming 3. Attack surface management 4. Phishing simulation 5. Either Digital Risk Management Services, OR both Anti-Phishing and Brand Protection & Monitoring Services 6. Dark web monitoring 7. Threat Intelligence feed 8. Threat Hunting services	a. Name of the Client. b. Date of Issue/Signing. c. Scope of Work demonstrating supply, installation and maintenance/AMC/support of the respective service. d. Solution Name and OEM Name OR Document 2: Client-Issued Supporting Document (Any-One) Any one of the following client-issued documents: a. Client Credential/Experience Certificate; or b. Email Confirmation from the Client; or c. Client-signed Installation/Implementation Report; or d. Client Acceptance/Go-Live/Completion/Sign-off Certificate; or e. AMC/Support Confirmation/Extension Letter The client-issued supporting document shall clearly establish, as applicable: • Name of the Client. • Project/service Name. • Successful Supply, Installation and Commissioning/Implementation. • Maintenance/Support/AMC status. • Date(s) establishing that the project falls within the required eligibility period. Note: If all the above information is not available in a single client-issued document, the Bidder may submit a combination of client-

#	Eligibility Criteria/Clause	Documents Required
		issued documents, provided that together they establish compliance with the eligibility criteria. AND Document 3: OEM's Self-Declaration (as per **Annexure 22B: OEM Self-Declaration For Implementation Experience)** The OEM shall submit a Self-Declaration cross-referencing the submitted documentary evidence and providing the following details: a. Project Name. b. Client Name. c. Client Category (PSU / PSE / Government Organization / BFSI) d. Scope Executed: a. Installation – Yes/No b. Maintenance / Under Maintenance – Yes/No e. Contract Period: a. Start Date b. End Date f. Service Name. g. OEM Name. h. Reference to the submitted client-issued document(s), including: a. Document Name. b. Relevant Page Number(s). c. Clause/Section/Page where the following are evidenced: i. Client Name. ii. Scope of Work. iii. Solution Name. iv. Maintenance/Support Status.

#	Eligibility Criteria/Clause	Documents Required
		v. Contract/Project Period.
24.	Compliance Confirmation from respective solution and services OEM Solution List: 1. SIEM 2. SOAR 3. UEBA 4. Extended Detection & response (XDR) 5. Decoy/Honey-Pot/Deception 6. Threat Intelligence Platform 7. Vulnerability assessment (VA) & vulnerability lifecycle management 8. Identity threat detection and response 9. Application Security testing Tool (SAST & DAST) 10. Cloud Security solution (CSPM) 11. CNAPP 12. CWPP 13. CTEM Services List: 1. Breach Attack & Simulation 2. Continuous Automated Red Teaming 3. Attack Surface management 4. Phishing simulation 5. Digital Risk management 6. Dark web monitoring 7. Threat Intelligence feed 8. Threat hunting services	Declaration in the format as mentioned in Annexure 18. FRS and TRS compliance sheet (Excel) are to be submitted along with the self-declaration.

#	Eligibility Criteria/Clause	Documents Required
25.	Functional Compliance: The Bidder's proposed solution shall be evaluated for functional compliance against the requirements specified in Appendix 1A: Functional Compliance Sheet. The proposed product should have minimum functional compliance score of 85% for each of the following: Solution List: 1. SIEM 2. SOAR 3. UEBA 4. Extended Detection & response (XDR) 5. Decoy/Honey-Pot/Deception 6. Threat Intelligence Platform 7. Vulnerability assessment (VA) & vulnerability lifecycle management 8. Identity threat detection and response 9. Application Security testing Tool (SAST & DAST) 10. Cloud Security solution (CSPM) 11. CNAPP 12. CWPP 13. CTEM Services List: 1. Breach Attack & Simulation 2. Continuous Automated Red Teaming 3. Attack Surface management 4. Phishing simulation	a) OEM Self Declaration (Annexure 32) b) Filled Appendix 1A & 1C: Functional Compliance Supporting Documentation like datasheets, product manuals, OEM website product feature listings etc. The Declaration is to be submitted by the OEMs of the following solution and services

<table>
<tr><th>#</th><th>Eligibility Criteria/Clause</th><th>Documents Required</th></tr>
<tr><td></td><td>
5. Digital Risk Management Services
6. Dark web monitoring
7. Threat Intelligence feed
8. Threat hunting services

Each product/solution shall be evaluated independently, and the compliance score shall be computed separately for each product/solution.

<table>
<tr><th>Maximum Marks</th><th>Compliance (S/C)</th><th>Maximum Mark</th></tr>
<tr><td>10</td><td>S (Standard):</td><td>This indicates that the requirement is covered by the standard product functionality. It includes features available out-of-the-box, as well as those achievable through parametrization or rules configuration.</td></tr>
<tr><td>3</td><td>C (Customization):</td><td>Requirements marked as "C" are the ones that require minor modifications to the proposed solution.
1. Such customizations may include development of custom code, creation of new interfaces, user interface enhancements, or</td></tr>
</table>
</td><td></td></tr>
</table>

#	Eligibility Criteria/Clause	Documents Required
	custom-built screens integrated with the base product. 2. All identified customizations shall be completed, tested, and made available by the bidder prior to commencement of User Acceptance Testing (UAT), without impacting the Bank's project timelines. 3. Only those changes that can be implemented without altering the base product and without impacting future upgrades, patches, or vendor support shall qualify as Customization (C)	

Note: In the event a Bidder participates in both the NextGen SOC RFP and IT Security solution & services RFP (GEM/2026/B/7936763 and GEM/2026/B/7752177) and is declared the successful bidder in either of the RFPs after completion of the commercial evaluation process, such Bidder shall be deemed ineligible for award in the other RFP. Accordingly, the commercial bid of such Bidder for the other RFP shall not be opened or, if already opened, shall not be considered for evaluation or award by the Bank. The decision of the Bank in this regard shall be final and binding.

a. Attested copies of all relevant documents, certificates, work orders, completion certificates, financial statements, and other supporting documents shall be submitted as documentary evidence in support of the claims made by the bidder. The bidder shall furnish any additional information and clarification as may be required by the Bank for verification of eligibility criteria. The Bank reserves the right to independently verify, evaluate, and validate the information and claims submitted by the bidder. The decision of the Bank in this regard shall be final, conclusive, and binding on the bidder.
b. In the event of a business transfer, acquisition, slump sale, merger, or acquisition of a business undertaking, the work experience, credentials, and references of the transferor entity ("Seller") pertaining to the acquired business may be considered, subject to submission of documentary evidence establishing such transfer and continuity of business operations.
c. In cases involving corporate restructuring, including merger, amalgamation, demerger, name change, conversion, or reorganization, the incorporation certificate, financial statements, work experience credentials, technical qualifications, and other relevant records of the predecessor entity may be considered, subject to submission of documentary evidence acceptable to the Bank.
d. Either the Principal/OEM or its authorized agent may submit a bid for a given item/product under this RFP. However, both the Principal/OEM and its authorized agent shall not be permitted to submit bids simultaneously for the same item/product in the same RFP. Further, where an agent is authorized to represent a Principal/OEM, the same agent shall not submit bids on behalf of more than one Principal/OEM for the same item/product under this RFP. Any violation of the above conditions shall render all such bids liable for rejection at the sole discretion of the Bank.
e. The bidder and/or OEM shall comply with applicable guidelines issued by the Central Vigilance Commission (CVC), including Circular No. 03/01/12, the applicable provisions of the General Financial Rules (GFR), and the Department of Expenditure Office Memorandum dated 25.07.2016, as amended from time to time.
f. In a tender, either the Indian Agent on behalf of the Principal/OEM or the Principal/OEM itself may bid; however, both shall not bid simultaneously for the same item/product in the same tender.
g. Documentary evidence shall be furnished against each eligibility criterion along with a detailed index of documents submitted. All documents shall be duly signed and stamped by the Authorized Signatory of the bidder. Relevant sections of the submitted documents supporting compliance with the eligibility criteria shall be clearly highlighted for ease of verification by the Bank.
h. Any misrepresentation, suppression of facts, submission of forged/fabricated documents, or provision of incorrect information by the bidder at any stage of the bidding process may result in rejection of the bid, forfeiture of bid security (if applicable), and/or blacklisting/debarment from participating in future procurement processes of the Bank, without prejudice to any other rights and remedies available to the Bank under law.
i. For the purpose of this RFP, the term "Scheduled Bank" shall exclude Regional Rural Banks (RRBs) and Payment banks. Accordingly, experience shall be considered for the purpose of evaluating eligibility and qualification criteria under this RFP.
j. Deployments shall be considered valid only if the solution has been used for its intended function in a production environment. Tests, pilot, or non-production deployments shall not be accepted.

k. Experience of solution(s) can be shown in single /multiple Clients/work orders meeting the criteria(s)
l. Experience should be during the five-year period preceding the RFP publication date. Even if the installation was completed more than five years ago, it will still qualify, provided the product is currently under maintenance or has been maintained at any time during the five-year period preceding the RFP publication date
m. Experience must be showcased separately for each solution category, with clear evidence that each solution has been deployed as a standalone solution and not merely as a feature or component of another solution.

When deemed necessary the Evaluation Committee may seek clarification on relevant aspects from the Bidder. However, that would not entitle the Bidder to change or cause any change. Bank reserves the right to conduct reference site visit/ video conference/ voice call with the Client to substantiate the credentials/ copy of PO/ Contract copy/ sign-off submitted by Bidder and/ or OEM. In case the input/ feedback received from the Customer is negative/ unsatisfactory, bank reserves the right to reject the Bid.

For and on behalf of [Full Legal Name of Bidder]

Authorized Signatory & Signature
Name: _____
Designation: _____
Signature: _____

16.6 Annexure 6: Acceptance/Compliance Certificate

RFP No.: _____ dated _____

(To be submitted by the Bidder on its official letterhead)

To
The General Manager (CISO)
Staff Training Centre
Punjab & Sind Bank
CISO Cell, 3rd Floor
B-8/232, Naharpur Village Road, Pocket 8, Sector 3B
Rohini, Delhi – 110085

Subject: Acceptance / Compliance Certificate

Dear Sir/Madam,

We, [Full Legal Name of Bidder / SI], hereby confirm that we have carefully read, understood and accepted all the terms and conditions, scope of work, technical and functional requirements, eligibility requirements, service levels, obligations and other provisions stipulated in RFP No. _____ dated _____, including all addenda, corrigenda, amendments, clarifications and communications issued by Punjab & Sind Bank from time to time.

We hereby undertake and confirm that:

1. Unconditional Acceptance: We unconditionally accept and agree to comply with all the requirements, terms and conditions of the RFP and shall execute the contract, SLAs and other terms in accordance with the RFP requirements.
2. Bidder confirms that all Terms and conditions have been duly vetted by the bidder's legal and bidder will sign the Contract, SLA and NDA as per the terms and condition stated in the RFP within 15 days of the PO Acceptance.
3. During the applicable support period, the bidder shall provide, as applicable, technical support, warranty/support services, software and firmware updates, security patches and fixes, vulnerability remediation/support, and availability of necessary spare parts/replacement components, in accordance with the OEM's applicable support policies and the requirements of the Tender. The bidder further confirms that the proposed Model(s) and Version(s) shall remain supportable and serviceable throughout the applicable support period, and the bidder shall provide necessary technical assistance for resolution of product-related technical and security issues during such period.
4. No Extraneous Conditions: Punjab & Sind Bank shall not be bound by any extraneous matter, assumption, condition, qualification, deviation or exclusion stated by us anywhere in our proposal or subsequently communicated by us, whether orally or in writing, unless specifically accepted by the Bank in writing.
5. Compliance with RFP: Any assumption, deviation, qualification or exclusion not expressly accepted by the Bank shall be deemed withdrawn and inapplicable, and we shall remain fully responsible for meeting the corresponding requirement of the RFP.
6. No Additional Cost: We shall make all necessary arrangements and provide all required resources, products, services, licences, infrastructure, support and other requirements

necessary for fulfilment of the RFP at no additional cost to the Bank, wherever such requirements are within the terms of the RFP.

7. Disqualification / Evaluation: We understand that any material deviation, exclusion, qualification or non-compliance may result in rejection/disqualification of our Bid, as per the provisions of the RFP.
8. Binding Nature: We acknowledge that the Bank's decision regarding acceptance or rejection of any assumption, deviation, exclusion or extraneous condition shall be final and binding on us.
9. We agree to submit the duly signed **NDA, Contract and SLA** within **15 (fifteen) days** from the date of acceptance of the Purchase Order (PO). In the event of failure to submit the duly signed documents within the stipulated period, the Bank shall have the right to take appropriate action in accordance with the terms and conditions of the RFP, **including forfeiture of the EMD and/or cancellation of the Purchase Order (PO) and/or any other as required in line with the terms of the RFP**.

We further confirm that our Bid is based on the requirements stipulated in the RFP, including all amendments, addenda, corrigenda and clarifications issued by the Bank, and that we shall fulfil all such requirements throughout the contract period.

We hereby certify that the above declaration is true and correct and undertake to comply with the same.

For and on behalf of [Full Legal Name of Bidder]

Authorized Signatory

Name: _____

Designation: _____

Signature: _____

Date: _____

Place: _____

Company Seal / Stamp

16.7 Annexure 7: Minimum Local Content Certification

Format for Affidavit of Self certification regarding Local Content in line with PPP-MII order and MoP Order, if applicable, to be provided on a non-judicial stamp paper of Rs. 100/-.

TENDER REREFENCE NUMBER: _____
Date:

To,

General Manager (Cyber Security)

STAFF TRAINING CENTRE PUNJAB AND SIND BANK

Punjab & Sind Bank, CISO cell 3rd Floor,

B-8/232, Naharpur Village Rd, Pocket 8, Sector 3B,

Rohini, Delhi, 110085

Dear Sir,

- This is to certify that proposed is having the local content of % as defined in the RFP.
- This certificate is submitted in reference to the Public Procurement (Preference to Make in India), Order 2017 – Revision vide Order No. P-45021/2/2017-PP (BE-II) dated June04, 2020.
- _____(Details of Locations where value additions are made).

Signature of Authorized Signatory
Name:
Date:
Designation:
Seal:

16.8 Annexure 8: Certification on OEM Requirements

RFP No.: _____

(Letter to be submitted on the OEM's letterhead from Security Solution & Services OEM)

To,
General Manager (CISO)
Staff Training Centre
Punjab & Sind Bank
CISO Cell, 3rd Floor
B-8/232, Naharpur Village Road, Pocket 8, Sector 3B
Rohini, Delhi – 110085

Subject: Request for Proposal for Selection of Bidder for Supply, Installation, Implementation, Maintenance & Management of NextGen SOC & Related Services vide RFP No. _____

Dear Sir/Madam,

We, [Full Legal Name of OEM], an established and reputable manufacturer/developer of [Product/Solution Name], having our registered office at [Address] and manufacturing/development facilities at [Address], confirm that we are the Original Equipment Manufacturer (OEM) of [Solution/Product Name, Product Family, Version/Edition] proposed by [Name of Bidder/SI] under the above-mentioned RFP.

We hereby confirm and undertake the following:

1. OEM Commitments
   - **a.** Scope of work pertaining to Requirement Analysis, System Design, Development & Implementation, Documentation, Final Deployment and Go-Live for our proposed product/solution shall be performed by us as specified in the RFP.
   - **b.** We shall provide our highest level of technical and product support during the O&M, Warranty, ATS and AMC phases, including applicable extension periods.
   - **c.** From Year 2 onwards, and annually thereafter during the Operations & Management phase, our personnel shall conduct a comprehensive review of configurations, rules, parameterizations and solution architecture for all PSB environments related to our product, in line with the defined requirement in the RFP. The review shall also cover relevant observations raised by regulators/auditors concerning implementation of our solution. A detailed report shall be submitted to the designated PSB SPOC by our assigned Project Manager/authorized representative.
   - **d.** We shall coordinate with the Bidder/SI for closure of observations identified in the review report and, where required, undertake closure through our personnel. Timelines for closure shall be discussed and agreed with the Bank based on the criticality of the observations.
   - **e.** The OEM shall provide the Bank with advance written notice of any material change, update, discontinuation, End-of-Sale (EoS), End-of-Life (EoL) or End-of-Support (EoS) event that may impact the Services. For any event likely to cause service disruption or discontinuity or materially impact the Services/SLAs, the OEM shall provide a minimum of six (6) months' prior written notice, wherever practicable, and support continuity/transition requirements.

f. We will provide two separate consoles for the proposed solution, one each from the DC and DR environments, to ensure and validate the functional readiness of both the DC and DR. We confirm that proposed product will be available for support for the period that is minimum 6 years.

2. Solution and Implementation Details

Particular	Details
Name of OEM	[●]
Name of Bidder / SI	[●]
Proposed Solution	[●]
Product / Platform Name	[●]
Product Version / Edition	[●]
Deployment Model	On-Premises / Cloud / Hybrid
Proposed Implementation Scope	[●]
Proposed Quantity / Capacity	[●]
License / Subscription Model	[●]
Support Model	[●]
Proposed Go-Live Date	[●]
Contract Period	[●]
Extension Period	[●]
OEM Support Contact / SPOC	[Name / Designation / Contact / Email]
Primary Site Location	[●]
Secondary Site Location	[●]
Management URL for Both DC & DR or OEM confirms they will perform and showcase DC/ DR drill before Go-Live	

3. Product Lifecycle and Latest Version Confirmation

We confirm that the product/version proposed under this RFP is the latest available production version as on the date of submission of the Bid.

We further confirm that the proposed product/version is not End-of-Sale (EoS), End-of-Life (EoL) or End-of-Support (EoS) as on the date of Bid submission and shall be supported by us throughout the required contract period, including the applicable extension period.

4. Replacement / Upgrade Undertaking

We confirm that if any software, hardware, appliance, subscription, license, component, module or other product supplied under this RFP becomes defective, unsupported, reaches EoL/EoS, underperforms, or fails to meet the specified functional, technical, capacity or performance requirements during the contract period, the OEM shall support the Bidder/Bank in repairing, replacing, upgrading or migrating the affected product/component with an equivalent or higher-capacity OEM-supported product/component, without disruption to the Bank's operations.

5. Cloud-Hosted Solution Confirmation (Cloud Hosted Solutions)

We confirm that there shall be no gap, ambiguity or conflict in ownership or accountability among the Bidder/SI, OEM and CSP for any obligation, service, security requirement, SLA, compliance requirement, data protection requirement or support obligation specified in the RFP.

The OEM shall remain responsible for all product-level implementation, designing, testing, Go-live, technical support, including product defects, patches, upgrades, vulnerabilities, product configuration, RCA, product performance and other OEM-specific obligations.

We confirm that all OEM commitments, obligations and dependencies required under this RFP have been secured and incorporated through appropriate agreements, support commitments, contractual arrangements and other binding mechanisms, as applicable.

6. Information Security, Privacy and Regulatory Compliance

We confirm that the proposed solution and services provided by the OEM shall comply with the Bank's applicable:

- Information Security requirements;
- Cyber Security requirements;
- Data Governance requirements;
- Data Retention requirements;
- Privacy and data protection requirements;
- Digital Personal Data Protection (DPDP) Act, as applicable;
- Applicable RBI, regulatory and statutory requirements;
- Bank's policies, standards and procedures; and
- Other contractual and security obligations specified in the RFP.

We shall provide necessary information, documentation, evidence, certifications, audit support and technical assistance required by the Bank for demonstrating such compliance.

7. OEM Support and SME Availability

We confirm that the OEM shall provide technical support and Subject Matter Expert (SME) support from the date of installation/deployment of the proposed solution throughout the contract period, including the applicable extension period.

OEM technical/SME support shall cover, at a minimum:

- Complex and major incident troubleshooting and resolution;
- Architecture assessment;
- Root Cause Analysis;
- Solution optimization and tuning;
- Configuration review;
- Product upgrades and migrations;
- Vulnerability remediation;
- Security updates and patches;
- Performance and capacity issues;
- Integration-related issues;
- Product defects and bugs;
- Technical audits and assessments; and
- Other technical requirements specified in the RFP.

The OEM shall ensure that appropriately qualified and experienced resources/SMEs are available within the timelines specified in the RFP/SLA.

8. Security Certificate post architecture assessment

The OEM's authorized representative Security Certificate to the Bank confirming:

The certificate shall confirm:

“All the proposed solutions and services are in good health, optimally configured, and operating at their required capacity and capabilities to ensure their intended effectiveness.”

Any exception, anomaly, security incident, degradation, capacity constraint, misconfiguration or known issue identified during the relevant period shall be reported to the Bank along with its impact, risk, corrective action and expected closure date.

9. Root Cause Analysis (RCA)

For all incidents related to the supplied solution, the OEM shall provide the Bidder/Bank with an OEM-issued RCA report within three (3) working days from the date of incident resolution, or within such other timeline as specified under the applicable SLA.

The RCA shall, at a minimum, include:

- Incident description and timeline;
- Root cause;
- Impact assessment;
- Technical analysis;
- Logs/evidence, wherever applicable;
- Corrective action taken;
- Preventive action proposed;
- Permanent resolution;
- Recommendations to prevent recurrence; and
- OEM closure confirmation.

10. OEM Accountability

We acknowledge that the solution proposed by [**Bidder Name**] is an OEM-supported solution and undertake to provide all necessary technical support, product support, lifecycle support, upgrades, patches, fixes and other OEM obligations specified in the RFP throughout the applicable contract period.

Any engagement, subcontracting, cloud hosting arrangement, distributor arrangement or third-party dependency associated with the proposed solution shall not dilute or transfer the OEM's obligations and commitments under this undertaking.

We confirm that the information provided in this undertaking is true and correct to the best of our knowledge and that the OEM shall honour the commitments contained herein and in the RFP.

For and on behalf of [OEM Legal Name]
Authorized Signatory
Name: _____
Designation: _____
Signature: _____

16.9 Annexure 9: Escalation Matrix

16.9.1 Annexure 9A: Escalation Matrix - Bidder

(Should be submitted on Company's letter head with company seal and signature of the authorized person)

Ref: RFP No._____ dated _____.

Name of the Company/Firm:

#	Name	Designation	Full Office Address	Phone No.	Mobile No.	Email address
a.		First Level Contact (Senior by designation to the project Director)				
b.		Second level contact (If response not received in 4 Hours)				
c.		Regional/Zonal Head (If response not received in 24 Hours)				
d.		Country Head (If response not received in 48 Hours)				

Any change in designation, substitution will be informed to bank immediately.

Date

Signature with seal

Name:

Designation:

16.9.2 Annexure 9B: Escalation Matrix – Respective security solution & service OEM

(Should be submitted on Company's letter head with company seal and signature of the authorized person)

Ref: RFP No._____ dated _____.

Name of the Company/Firm:

#	Name	Designation	Full Office Address	Phone No.	Mobile No.	Email address
e.		First Level Contact (Senior by designation to the project Director)				
f.		Second level contact (If response not received in 4 Hours)				
g.		Regional/Zonal Head (If response not received in 24 Hours)				
h.		Country Head (If response not received in 48 Hours)				

Any change in designation, substitution will be informed to bank immediately.

Date

Signature with seal

Name:

Designation:

16.10 Annexure 10: Litigation Certificate

Litigation Certificate

Reg.: Selection of Bidder(s) For Request for proposal for Selection of bidder for supply installation, implementation, maintenance & management of NextGen SOC & related services

To be provided by Statutory Auditor/Chartered Accountant

This is to certify that M/s_____, a company incorporated under the companies act, 1956 with its headquarters at, _____ is not involved in any litigation which threatens solvency of the company.

Date: _____

Place: _____

Signature of CA/Statutory Auditor

Name of CA/Statutory Auditor:

Designation:

Email ID:

Mobile No:

Telephone No.:

Seal of Company:

16.11 Annexure 11: Non-blacklisting undertaking

Undertaking for non-blacklisting

To,

General Manager (CISO)

STAFF TRAINING CENTRE PUNJAB AND SIND BANK

Punjab & Sind Bank, CISO cell 3rd Floor,

B-8/232, Naharpur Village Rd, Pocket 8, Sector 3B,

Rohini, Delhi, 110085

Dear Sir,

Reg.: Request for proposal for Selection of bidder for supply installation, implementation, maintenance & management of NextGen SOC & related services

We M/s_____, a company incorporated under the companies act, 1956 with its headquarters at, _____ do hereby confirm that we have not been blacklisted/ debarred by the Government / Government agency / Banks / Financial Institutions in India during last 3 years.

This declaration has been submitted and limited to, in response to the tender reference mentioned in this document

Thanking You,

Yours faithfully,

Date: _____

Place: _____

Signature of Authorized Signatory

Name of Signatory:

Designation:

Email ID:

Mobile No:

Telephone No.:

Seal of Company:

16.12 Annexure 12: Undertaking of Authenticity (on bidder's letterhead)

To:

General Manager (CISO)
STAFF TRAINING CENTRE PUNJAB AND SIND BANK
Punjab & Sind Bank, CISO cell 3rd Floor,
B-8/232, Naharpur Village Rd, Pocket 8, Sector 3B,
Rohini, Delhi, 110085

Sub: Undertaking of Authenticity for supplied Product(s)

Ref: RFP No. xx:xx dated dd/mm/yyyy

With reference to the Product being quoted to you vide our Bid No:_____ dated _____, we hereby undertake that all the components /parts /assembly / software etc. used in the Product to be supplied shall be original new components / parts / assembly / software only, from respective Original Equipment Manufacturers (OEMs) of the Products and that no refurbished / duplicate / second hand components /parts/ assembly / software shall be supplied or shall be used or no malicious code are built-in in the Product being supplied.

1. We also undertake that in respect of licensed operating systems and other software utilities to be supplied, the same will be sourced from authorized sources and supplied with Authorized License Certificate (i.e. Product keys on Certification of Authenticity in case of Microsoft Windows Operating System).

2. Should you require, we hereby undertake to produce the certificate from our OEM supplier in support of above undertaking at the time of delivery/installation. It will be our responsibility to produce such letters from our OEM supplier's at the time of delivery or within a reasonable time.

3. In case of default and/or the Bank finds that the above conditions are not complied with, we agree to take back the Product(s) supplied and return the money paid by you, in full within seven days of intimation of the same by the Bank, without demur or any reference to a third party and without prejudice to any remedies the Bank may deem fit.

4. We also take full responsibility of both Product(s) & Service(s) as per the content of the RFP even if there is any defect by our authorized Service Centre / Reseller / SI etc.

Dated this ..... day of 2026

(Signature)

(Name)

(In the capacity of)

Duly authorised to sign Bid for and on behalf of _____

16.13 Annexure 13: Non-Disclosure Agreement

NON-DISCLOSURE AGREEMENT

All bidders must sign the Non-Disclosure Agreement (NDA) while submitting the response to the Request for proposal (RFP). Bidders must comply with all clauses mentioned in the NDA. No changes to the NDA are allowed.

NDA format is provided below.

(To be stamped in accordance with stamp act)

Strictly Private and Confidential

This Non-Disclosure Agreement made and entered into at……. This ……..day……of……..20……BY AND BETWEEN …… ……., a company incorporated under the Companies Act, 1956 having its registered office at ……. (Hereinafter referred to as the Bidder which expression unless repugnant to the context or meaning thereof be deemed to include its permitted successors) of the ONE PART;

AND

Punjab & Sind Bank, a body corporate, established under the Banking Companies (Acquisition and Transfer of Undertakings) Act 1980 and having its ……(hereinafter referred to as "Bank" which expression shall unless it be repugnant to the subject, meaning or context thereof, be deemed to mean and include its successors and assigns) of the OTHER PART.

The Bidder and Punjab & Sind Bank are hereinafter collectively referred to as "the Parties" and individually as "the Party".

WHEREAS:

1. Punjab & Sind Bank is engaged in the business of providing financial services to its customers and intends to engage service provider _____
2. In the course of such an assignment, it is anticipated that Punjab & Sind Bank or any of its officers, employees, officials, representatives or agents may disclose, or deliver, to the Bidder some Confidential Information (as hereinafter defined), to enable the Bidder to carry out the aforesaid Implementation assignment (hereinafter referred to as " the Purpose").
3. The Bidder is aware and confirms that all information, data and other documents made available in the RFP/Bid Documents/Agreement /Contract or in connection with the Services rendered by the Bidder are confidential information and are privileged and strictly confidential and or proprietary of Punjab & Sind Bank. The Bidder undertakes to safeguard and protect such confidential information as may be received from Punjab & Sind Bank.

NOW, THEREFORE THIS AGREEMENT WITNESSED THAT in consideration of the above premises and the Punjab & Sind Bank granting the Bidder and or his agents, representatives to have specific access to Punjab & Sind Bank property / information and other data it is hereby agreed by and between the parties hereto as follows:

4. Confidential Information:
   i. "Confidential Information" means all information disclosed/furnished by Punjab & Sind Bank to the Bidder whether orally, in writing or in electronic, magnetic or other form for the limited purpose of enabling the Bidder to carry out the proposed Implementation assignment, and shall mean and include data, documents and information or any copy, abstract, extract, sample, note or module thereof, explicitly designated as "Confidential"; Provided the oral information is set forth in writing and marked "Confidential" within seven (7) days of such oral disclosure.
   ii. The Bidder may use the Confidential Information solely for and in connection with the Purpose and shall not use the Confidential Information or any part thereof for any reason other than the Purpose stated above.

Confidential Information in oral form must be identified as confidential at the time of disclosure and confirmed as such in writing within seven (7) days of such disclosure. Confidential Information does not include information which:

a) is or subsequently becomes legally and publicly available without breach of this Agreement by either party,
b) was rightfully in the possession of the Bidder without any obligation of confidentiality prior to receiving it from Punjab & Sind Bank,
c) was rightfully obtained by the Bidder from a source other than Punjab & Sind Bank without any obligation of confidentiality,
d) was developed by for the Bidder independently and without reference to any Confidential Information and such independent development can be shown by documentary evidence, or is/was disclosed pursuant to an order of a court or governmental agency as so required by such order, provided that the Bidder shall, unless prohibited by law or regulation, promptly notify Punjab & Sind Bank of such order and afford Punjab & Sind Bank the opportunity to seek appropriate protective order relating to such disclosure.
e) the recipient knew or had in its possession, prior to disclosure, without limitation on its confidentiality.
f) is released from confidentiality with the prior written consent of the other party.

The recipient shall have the burden of proving hereinabove are applicable to the information in the possession of the recipient. Confidential Information shall at all times remain the sole and exclusive property of the disclosing party. Upon termination of this Agreement, Confidential Information shall be returned to the disclosing party or destroyed, if incapable of return. The destruction shall be witnessed and so recorded, in writing, by an authorized representative of each of the parties.

Nothing contained herein shall in any manner impair or affect the rights of Punjab & Sind Bank in respect of the Confidential Information.

In the event that any of the Parties hereto becomes legally compelled to disclose any Confidential Information, such Party shall give sufficient notice to the other party to enable the other Party to prevent or minimize to the extent possible, such disclosure. Neither party shall disclose to a third party any Confidential Information or the contents of this Agreement without the prior written consent of the other party. The obligations of this Clause shall be satisfied by handling

Confidential Information with the same degree of care, which the receiving party applies to its own similar confidential information but in no event less than reasonable care.

The obligations of this clause shall survive the expiration, cancellation or termination of this Agreement and for a period of five (5) years with respect to project confidentiality. However, confidentiality obligations with respect to individually identifiable information, data/ information classified as PII, any customer's data of bank and any IPR of the bank shall survive in perpetuity.

5. Non-disclosure: The Bidder shall not commercially use or disclose any Confidential Information, or any materials derived there from to any other person or entity other than persons in the direct employment of the Bidder who have a need to have access to and knowledge of the Confidential Information solely for the Purpose authorized above. The Bidder shall take appropriate measures by instruction and written agreement prior to disclosure to such employees to assure against unauthorized use or disclosure. The Bidder may disclose Confidential Information to others only if the Bidder has executed a Non-Disclosure Agreement with the other party to whom it is disclosed that contains terms and conditions that are no less restrictive than these presents, and the Bidder agrees to notify Punjab & Sind Bank immediately if it learns of any use or disclosure of the Confidential Information in violation of terms of this Agreement.

Notwithstanding the marking and identification requirements above, the following categories of information shall be treated as Confidential Information under this Agreement irrespective of whether it is marked or identified as confidential:

a) Information regarding Punjab & Sind Bank and any of its Affiliates, customers and their accounts ("Customer Information"). For purposes of this Agreement, Affiliate means a business entity now or hereafter controlled by, controlling or under common control. Control exists when an entity owns or controls more than 10% of the outstanding shares or securities representing the right to vote for the election of directors or other managing authority of another entity; or
b) any aspect of Punjab & Sind Bank's business that is protected by patent, copyright, trademark, trade secret or other similar intellectual property right; or
c) business processes and procedures; or
d) current and future business plans; or
e) personnel information; or
f) Financial information.

6. Publications: The Bidder shall not make news releases, public announcements, give interviews, issue or publish advertisements or publicize in any other manner whatsoever in connection with this Agreement, the contents / provisions thereof, other information relating to this Agreement, the Purpose, the Confidential Information or other matter of this Agreement, without the prior written approval of Punjab & Sind Bank.
7. Term: This Agreement shall be effective from the date hereof and shall continue till expiration of the Purpose or termination of this Agreement by Punjab & Sind Bank, whichever is earlier. The Bidder hereby agrees and undertakes to Punjab & Sind Bank that immediately on termination of this Agreement it would forthwith cease using the Confidential Information and further promptly return or destroy, under

information to Punjab & Sind Bank, all information received by it from Punjab & Sind Bank for the Purpose, whether marked Confidential or otherwise, and whether in written, graphic or other tangible form and all copies, abstracts, extracts, samples, notes or modules thereof. The Bidder further agree and undertake to Punjab & Sind Bank to certify in writing upon request of Punjab & Sind Bank that the obligations set forth in this Agreement have been complied with.

Any provisions of this Agreement which by their nature extend beyond its termination shall continue to be binding and applicable without limit in point in time except and until such information enters the public domain

8. Title and Proprietary Rights: Notwithstanding the disclosure of any Confidential Information by Punjab & Sind Bank to the Bidder, the title and all intellectual property and proprietary rights in the Confidential Information shall remain with Punjab & Sind Bank.
9. Remedies: The Bidder acknowledges the confidential nature of Confidential Information and that damage could result to Punjab & Sind Bank if the Bidder breaches any provision of this Agreement and agrees that, if it or any of its directors, officers or employees should engage or cause or permit any other person to engage in any act in violation of any provision hereof, Punjab & Sind Bank may suffer immediate irreparable loss for which monetary compensation may not be adequate. Punjab & Sind Bank shall be entitled, in addition to other remedies for damages & relief as may be available to it, to an injunction or similar relief prohibiting the
10. Bidder, its directors, officers etc. from engaging in any such act which constitutes or results in breach of any of the covenants of this Agreement.
11. Any claim for relief to Punjab & Sind Bank shall include Punjab & Sind Bank's costs and expenses of enforcement (including the attorney's fees).
12. Entire Agreement, Amendment and Assignment: This Agreement constitutes the entire agreement between the Parties relating to the matters discussed herein and supersedes any and all prior oral discussions and / or written correspondence or agreements between the Parties. This Agreement may be amended or modified only with the mutual written consent of the Parties. Neither this Agreement nor any right granted hereunder shall be assignable or otherwise transferable.
13. Dispute Resolution: If any dispute, difference or claim arises between the parties hereto in connection with the validity, interpretation, implementation or alleged breach of the terms of this Agreement or anything done or omitted to be done pursuant to this Agreement, the Parties shall attempt in the first instance to resolve the same through negotiation. If the dispute is not resolved through negotiation within 30 (thirty) days after commencement of discussions, then, the parties shall be at liberty to approach competent court of law at Delhi for adjudication of the disputes.
14. Governing Law: Governing Law: The laws of India shall govern this Agreement
15. Jurisdiction: It is hereby agreed between the parties that any suit or legal proceedings to enforce the rights of either party under this Agreement shall be instituted and tried by a competent court in the city of Delhi only.
16. Authorized Signatory: The selected Bidder shall indicate the authorized signatories who can discuss and correspond with the bank about the obligations under the contract. The selected Bidder shall submit at the time of signing the contract a certified copy of the resolution of their board, authenticated by the company secretary, authorizing an official or officials of the Bidder to discuss, sign agreements/contracts with The Bank, raise invoice and accept payments and also to

correspond. The Bidder shall provide proof of signature identification for the above purposes as required by the bank

17. Force Majeure: Force Majeure is herein defined as any cause, which is beyond the control of the selected Bidder or The Bank as the case may be which they could not foresee or with a reasonable amount of diligence could not have foreseen and which substantially affect the performance of the contract, such as:-

- Natural phenomenon, including but not limited to floods, droughts, earthquakes, epidemics and pandemics
- Acts of any government, including but not limited to war, declared or undeclared priorities, quarantines and embargos
- Terrorist attack, public unrest in work area
- Provided either party shall within 10 days from occurrence of such a cause, notify the other in writing of such causes. The Bidder or The Bank shall not be liable for delay in performing his/her obligations resulting from any force Majeure cause as referred to and/or defined above. Any delay beyond 30 days shall lead to termination of contract by parties and all obligations expressed quantitatively shall be calculated as on date of termination. Notwithstanding this, provisions related to indemnity, confidentiality survive termination of the contract.
- Unless otherwise directed by the bank in writing, the Bidder affected by force majeure shall continue to perform the obligations under this agreement, which are not affected by the force majeure event and shall take such steps as are reasonably necessary to remove the causes resulting in force majeure and to mitigate the effect thereof.
- As soon as the cause of force majeure has been removed, the Bidder shall notify the Bank and resume the affected activity without delay.
- Notwithstanding the above, the decision of the bank shall be final and binding on the Bidder in the event of force majeure.

18. Intellectual Property Indemnity: In the event of any claim asserted by a third party of infringement of copyright, patent, trademark, industrial design rights, etc., arising from the use of the Goods or any part thereof in India, the Vendor(s) shall act expeditiously to extinguish such claim. If the Vendor(s) fails to comply and the Bank is required to pay compensation to a third party resulting from such infringement, the Vendor(s) shall be responsible for the compensation to the claimant including all expenses, court costs and lawyer fees. The Bank will give notice to the Vendor(s) of such a claim, if it is made, without delay. The Vendor(s) shall indemnify the Bank against all third-party claims.
19. General: The Bidder shall not reverse - engineer, decompile, disassemble or otherwise interfere with any software disclosed hereunder.
20. All Confidential Information is provided “as is”. In no event shall the Punjab & Sind Bank be liable for the inaccuracy or incompleteness of the Confidential Information. None of the Confidential Information disclosed by Punjab & Sind Bank constitutes any representation, warranty, assurance, guarantee or inducement with respect to the fitness of such Confidential Information for any particular purpose.
21. Punjab & Sind Bank discloses the Confidential Information without any representation or warranty, whether express, implied or otherwise, on truthfulness, accuracy, completeness, lawfulness, merchant ability, fitness for a particular purpose, title, non-infringement, or anything else.

22. Waiver: A waiver (whether express or implied) by Punjab & Sind Bank of any of the provisions of this Agreement, or of any breach or default by the Bidder in performing any of the provisions hereof, shall not constitute a continuing waiver and such waiver shall not prevent Punjab & Sind Bank from subsequently enforcing any of the subsequent breach or default by the Bidder under any of the provisions of this Agreement.

In witness whereof, the Parties hereto have executed these presents the day, month and year first herein above written.

For and on behalf of _____	For and on behalf of Punjab & Sind Bank

16.14 Annexure 14: Commercial Proposal Submission Checklist

Instructions to be noted while preparing/submitting Commercial Proposal

All Annexure or appendix should be submitted in Bidder's Letter Head with seal and signature of the authorized signatory.

1. Bill of Material as per Appendix 2.

16.15 Annexure 15: Bank Guarantee Format for Earnest Money Deposit

Performa for the Bank Guarantee for Earnest Money Deposit

(To be stamped in accordance with stamp act)

Ref: Bank Guarantee #

Date: _____

To,

General Manager (CISO)

STAFF TRAINING CENTRE PUNJAB AND SIND BANK

Punjab & Sind Bank, CISO cell 3rd Floor,

B-8/232, Naharpur Village Rd, Pocket 8, Sector 3B,

Rohini, Delhi, 110085

Dear Sir,

In accordance with your bid reference No._____Dated _____M/s_____ having its registered office at _____herein after Called „bidder") wish to participate in the said bid for Selection of Bidder(s) Selection of bidder for supply installation, implementation, maintenance & management of NextGen SOC & related services An irrevocable Financial Bank Guarantee (issued by a nationalized /scheduled commercial Bank) against Earnest Money Deposit amounting to Rs.....) valid up to _____ is required to be submitted by the bidder, as a condition for participation in the said bid, which amount is liable to be forfeited on happening of any contingencies mentioned in the bid document. M/s_____ having its registered office at _____ has undertaken in pursuance of their offer to Punjab & Sind Bank (hereinafter called as the beneficiary) dated _____ has expressed its intention to participate in the said bid and in terms thereof has approached us and requested us_____ (Name of Bank) _____ (Address of Bank) to issue an irrevocable financial Bank Guarantee against Earnest Money Deposit (EMD) amounting to Rs _____(Rupees_____) valid up to_____. We, the _____ (Name of Bank)_____ (Address of Bank) having our Head office at _____ therefore Guarantee and undertake to pay immediately on first written demand by Punjab & Sind, the amount Rs. _____(Rupees_____) without any reservation, protest, demur and recourse in case the bidder fails to Comply with any condition of the bid or any violation against the terms of the bid, Without the beneficiary needing to prove or demonstrate reasons for its such demand. Any Such demand made by said beneficiary shall be conclusive and binding on us irrespective of any dispute or difference raised by the bidder. This guarantee shall be irrevocable and shall remain valid up to _____. If any further extension of this Guarantee is required, the same shall be extended to such required period on receiving instructions in writing, from Punjab & Sind Bank, on whose behalf guarantee is issued. "Not

withstanding anything contained herein above Our liability under this bank guarantee shall not exceed Rs._____ (Rupees_____).

This bank guarantee shall be valid up to _____. We are liable to pay the guaranteed amount or any part thereof under this bank guarantee only if you serve upon us a written claim or demand, on or before _____14.30 hours (Indian Standard Time) or within Bank official working hours where after it ceases to be in effect in all respects whether or not the original bank guarantee is returned to us." In witness whereof the Bank, through its authorized officer has set its hand stamped on this _____ Day of _____2026 at _____

Name of signatory

Bank Common Seal

Designation

16.16 Annexure 16: Format of Performance Guarantee

(Issued by any Scheduled Commercial Bank & to be executed on stamp paper of requisite value as per stamp duty payable at place of execution.)

Tender Reference No: _____ Date _____

To,

General Manager (CISO)

STAFF TRAINING CENTRE PUNJAB AND SIND BANK

Punjab & Sind Bank, CISO cell 3rd Floor,

B-8/232, Naharpur Village Rd, Pocket 8, Sector 3B,

Rohini, Delhi, 110085

Dear Sir,

1. WHEREAS pursuant to a Request for Proposal dated…….. (hereinafter referred to as RFP, issued by Punjab & Sind Bank, Staff Training Centre Punjab & Sind Bank, B-8/232, Naharpur Village Rd, Pocket 8, Sector 3B,Rohini, Delhi, 110085 in response of (Bidder(s) / Service Provider), a Company registered under the Companies Act, 1956 and having its Registered / Corporate Office at ……has awarded the Contract valued Rs…….and appointed……..as Bidder(s) / Service Provider for procurement of ……vide Appointment letter / Purchase Order No……dated……..on the terms and conditions as set out inter-alia in the said RFP and in the Appointment Letter / Purchase Order.

2. WHEREAS you have in terms of the said Appointment letter / Purchase Order called upon (Bidder(s) / Service Provider to furnish a Performance Guarantee, for Rs…….Rupees only), equivalent to……..of the Contract value, to be issued by a Bank in your favour towards due performance of the Contract in accordance with the specifications, terms and conditions of the said Appointment letter / Purchase Order and an Agreement entered / to be entered into in this behalf.
3. WHEREAS (Bidder(s) / Service Provider) has approached us for issuing in your favour a performance Guarantee for the sum of Rs…….. (Rupees…….).
   NOW THEREFORE in consideration of you having awarded the Contract to…..…….inter-alia on the terms & conditions that provides a performance guarantee for due performance of the terms and conditions thereof. We,…….Bank,…… a body corporate constituted under ……having its Head office at……(give full address) and a branch inter-alia at…….. India at the request of……do hereby expressly, irrevocably and unconditionally undertake to pay merely on demand from you and without any demur without referring to any other source, Rs…….(Rupees……only) against any loss or

damage caused to or suffered by or that may be caused to or suffered by you on account of any breach or breaches on the part of ……of any of the terms and conditions of the Contract and in the event of……committing any default or defaults in carrying out any of the work or discharging any obligation under the said Contract or otherwise in the observance and performance of any of the terms and conditions relating thereto including non-execution of the Agreement as may be claimed by you on account of breach on the part of …….of their obligations or default in terms of the said Appointment letter / Purchase Order.

4. Notwithstanding anything to the contrary contained herein or elsewhere, we agree that your decision as to whether the ……..has committed any such breach / default or defaults and the amount or amounts to which you are entitled by reasons thereof will be binding on us and we shall not be entitled to ask you to establish its claim or claims under this Guarantee, but will pay the same forthwith on demand without any protest or demur. Any such demand made by you shall be conclusive as regards the amount due and payable by us to you.
5. This Guarantee shall be valid up to …….. plus 12 months of the Claim period from the expiry of said guarantee period. Without prejudice to your claim or claims arisen and demanded from or otherwise notified to us in writing before the expiry of the said date which will be enforceable against us notwithstanding that the same is or are enforced after the said date.
6. You will have the fullest liberty without our consent and without affecting our liabilities under this Guarantee from time to time to vary any of the terms and conditions of the said appointment letter or the Contract to be made pursuant thereto or extend the time of performance of the Contract or to postpone for any time or from time to time any of your rights or powers against the ……and either to enforce or forbear to enforce any of the terms and conditions of the said appointment letter or the Contract and we shall not be released from our liability under Guarantee by exercise of your liberty with reference to matters aforesaid or by reason of any time being given to or any other forbearance, act or omission on your part or any indulgence by you or any other act, matter or things whatsoever which under law relating to sureties, would but for the provisions hereof have the effect of releasing us from our liability hereunder provided always that nothing herein contained will enlarge our liability hereunder beyond the limit of Rs…….. (Rupees……only) as aforesaid or extend the period of the guarantee beyond ……(date) unless expressly agreed to by us in writing.
7. This Guarantee shall not in any way be affected by you are taking or giving up any securities from ……or any other person, firm or company on its behalf or by the winding up, dissolution, insolvency as the case may be of …….
8. In order to give full effect to the Guarantee herein contained, you shall be entitled to act as if we were your principal debtors in respect of all your claims against …….hereby guaranteed by us as aforesaid and we hereby expressly waive all our rights of surety ship and other rights, if any, which are in any way inconsistent with any of the provisions of Guarantee.
9. Subject to the maximum limit of our liability as aforesaid, this Guarantee will cover all your claim or claims against ……from time to time arising out of or in relation to the said appointment letter / Contract and in respect of which your claim in writing is lodged on us before expiry of Guarantee.

10. Any Notice by way of demand or otherwise hereunder may be sent by special courier, telex, fax, e-mail or registered post to our Head Office / Local address as aforesaid and if sent accordingly it shall be deemed to have been given when the same has been posted.
11. This Guarantee shall not be affected by any change in the constitution of _____or nor shall it be affected by any change in your constitution or by any amalgamation or absorption thereof or therewith but will ensure to the benefit of and be available to and be enforceable by the absorbing or amalgamated company or concern.
12. This Guarantee shall come into force from the date of its execution and shall not be revoked by us any time during its currency without your previous consent in writing.
13. We further agree and undertake to pay you the amount demanded in writing irrespective of any dispute or controversy between you and _____ in any suit or proceeding pending before any court, Tribunal or Arbitrator relating thereto, our liability under these presents being absolute and unequivocal. The payments so made by us shall be a valid discharge of our liability for payment hereunder and _____shall have no claim against us for making such payment.
14. We have the power to issue this Bank Guarantee in your bank's favour as the undersigned has full power to execute this Bank Guarantee under the Power of Attorney issued by our Bank.
15. Our authority to issue this guarantee may be verified with our Controlling Office situated at _____ (full details of persons to be contacted address and phone Numbers etc).
16. Notwithstanding anything contained herein above;
    i. Our liability under this Guarantee shall not exceed Rs_____(Rupees_____only)
    ii. This Guarantee shall be valid and remain in force up to_____ plus the Claim period of 12(Twelve) months and including the date _____ and
    iii. We are liable to pay the guaranteed amount or any part thereof under this Guarantee only and only if you serves upon us a written claim or demand for payment on or before the expiry of this Guarantee. ss

Dated this the_____ day of _____ 2026

Signature and Seal of Guarantors

Bidder(s)'s Bank

16.17 Annexure 17 : Pre-contract integrity pact

(To be stamped in accordance with stamp act)

PRE-CONTRACT INTEGRITY PACT

Between

Punjab & Sind Bank (PSB) hereinafter referred to as "The Principal",

And

_____ hereinafter referred to as "The Bidder/ Contractor"

Preamble

The Principal intends to award, under laid down organizational procedures, contract/ s for _____ _____. The Principal values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness / transparency in its relations with its Bidder(s) and / or Contractor(s).

In order to achieve these goals, the Principal has appointed 1. Sh. Debal kumar Gayen Gayen.dk@gmail.com 2. Sh. Pramod Kumar Garg Pkgarg.1957@gmail.com as Independent External Monitors (IEMs) who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

Section 1 - Commitments of the Principal

(1) The Principal commits itself to take all measures necessary to prevent corruption and to observe the following principles: -

a. No employee of the Principal, personally or through family members, will in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

b. The Principal will, during the tender process treat all Bidder(s) with equity and reason. The Principal will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential / additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution.

c. The Principal will exclude from the process all known prejudiced persons.

(2) If the Principal obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions

Section 2 - Commitments of the Bidder(s)/ Contractor(s)

(1) The Bidder(s)/ Contractor(s) commit themselves to take all measures necessary to prevent corruption. The Bidder(s)/ Contractor(s) commit themselves to observe the following principles during participation in the tender process and during the contract execution.

a. The Bidder(s)/ Contractor(s) will not, directly or through any other person or firm, offer, promise or give to any of the Principal's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he / she is not legally entitled to, in order to obtain in exchange any advantage of an kind whatsoever during the tender process or during the execution of the contract.

b. The Bidder(s)/ Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications,

certifications, subsidiary contract submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelisation in the bidding process.

c. The Bidder(s)/ Contractor(s) will not commit any offence under the relevant IPC/PC Act; further the Bidder(s)/ Contractor(s) will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

d. The Bidder(s)/Contractors(s) of foreign origin shall disclose the name and address of the Agents/representatives in India, if any, similarly the Bidder(s)/Contractors(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any. Further details as mentioned in the "Guidelines on Indian Agents of Foreign Suppliers" shall be disclosed by the Bidder(s)/Contractor(s). Further, as mentioned in the Guidelines all the payments made to the Indian agent/representative have to be in Indian Rupees only.

e. The Bidder(s)/ Contractor(s) will, when presenting their bid, disclose any and all payments made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract.

f. Bidder(s) /Contractor(s) who have signed the Integrity Pact shall not approach the Courts while representing the matter to IEMs and shall wait for their decision in the matter.

(2) The Bidder(s)/ Contractor(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section 3 - Disqualification from tender process and exclusion from future contracts

If the Bidder(s)/Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or in any other form such as to put their reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s)/Contractor(s) from the tender process or take action as per the procedure mentioned in the "Guidelines on Banning of business dealings".

Section 4 - Compensation for Damages

(1) If the Principal has disqualified the Bidder(s) from the tender process prior to the award according to Section 3, the Principal is entitled to demand and recover the damages equivalent to Earnest Money Deposit/ Bid Security.

(2) If the Principal has terminated the contract according to Section 3, or if the Principal is entitled to terminate the contract according to Section 3, the Principal shall be entitled to demand and recover from the Contractor liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee.

Section 5 - Previous transgression

(1) The Bidder declares that no previous transgressions occurred in the last three years with any other Company in any country conforming to the anti-corruption approach or with any Public Sector Enterprise in India that could justify his exclusion from the tender process.

(2) If the Bidder makes incorrect statement on this subject, he can be disqualified from the tender process or action can be taken as per the procedure mentioned in "Guidelines on Banning of business dealings".

Section 6 - Equal treatment of all Bidders /Contractors / Subcontractors

(1) In case of Sub-contracting, the Principal Contractor shall take the responsibility of the adoption of Integrity Pact by the Sub-contractor.

(2) The Principal will enter into agreements with identical conditions as this one with all Bidders and Contractors.

(3) The Principal will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

Section 7 - Criminal charges against violating Bidder(s) / Contractor(s) / Subcontractor(s)

If the Principal obtains knowledge of conduct of a Bidder, Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if the Principal has substantive suspicion in this regard, the Principal will inform the same to the Chief Vigilance Officer.

Section 8 - Independent External Monitor

(1) The Principal appoints competent and credible Independent External Monitor for this Pact after approval by Central Vigilance Commission. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.

(2) The Monitor is not subject to instructions by the representatives of the parties and performs his/her functions neutrally and independently. The Monitor would have access to all Contract documents, whenever required. It will be obligatory for him / her to treat the information and documents of the Bidders/Contractors as confidential. He/ she reports to the MD & CEO of Punjab & Sind Bank.

(3) The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the Principal including that provided by the Contractor. The Contractor will also grant the Monitor, upon his/her request and demonstration of a valid interest, unrestricted and unconditional access to their project documentation. The same is applicable to Sub-contractors.

(4) The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/ Contractor(s)/ Sub-contractor(s) with confidentiality. The Monitor has also sighed declarations on 'Non-Disclosure of Confidential Information' and of 'Absence of Conflict of Interest'. In case of any conflict of interest arising at a later date, the IEM shall inform MD & CEO of Punjab & Sind Bank and recuse himself / herself from that case.

(5) The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Contractor. The parties offer to the Monitor the option to participate in such meetings.

(6) As soon as the Monitor notices, or believes to notice, a violation of this agreement, he/she will so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.

(7) The Monitor will submit a written report to the MD & CEO of Punjab & Sind Bank, within 8 to 10 weeks from the date of reference or intimation to him by the Principal and, should the occasion arise, submit proposals for correcting problematic situations.

(8) If the Monitor has reported to the MD & CEO of Punjab & Sind Bank, a substantiated suspicion of an offence under relevant IPC/ PC Act, and the MD & CEO of Punjab & Sind Bank has not, within the reasonable time taken visible action to proceed against such offence or reported it to

the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

(9) The word 'Monitor' would include both singular and plural

Section 9 - Pact Duration

This Pact begins when both parties have legally signed it. It expires for the Contractor 12 months after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded. Any violation of the same would entail disqualification of the bidders and exclusion from future business dealings.

If any claim is made / lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged / determined by MD & CEO of Punjab & Sind Bank.

Section 10 - Other provisions

(1) This agreement is subject to Indian Law. Place of performance and jurisdiction is the Registered Office of the Principal, i.e. New Delhi.

(2) Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.

(3) If the Contractor is a partnership or a consortium, this agreement must be signed by all partners or consortium members.

(4) Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

(5) Issues like Warranty / Guarantee etc. shall be outside the purview of IEMs.

(6) In the event of any contradiction between the Integrity Pact and its Annexure, the Clause in the Integrity Pact will prevail.

_____

(For & On behalf of the Principal) (For & On behalf of Bidder / Contractor)

Place ----------

Date ----------

Witness 1:

(Name & Address)

Witness 2:

(Name & Address)

16.18 Annexure 18: Compliance with FRS, TRS, SoW & SBOM (on respective OEM letterhead)

RFP No:

(Letter to be submitted by the OEMs on their letter head from Security Solutions, Services, IT Hardware, Backup Software OEMs)

To,

General Manager (CISO)

STAFF TRAINING CENTRE PUNJAB AND SIND BANK

Punjab & Sind Bank, CISO cell 3rd Floor,

B-8/232, Naharpur Village Rd, Pocket 8, Sector 3B,

Rohini, Delhi, 110085

Dear Sir,

Sub: Request for proposal for selection of bidder(s) for procurement of Selection of bidder for supply installation, implementation, maintenance & management of NextGen SOC & related services vide RFP No: _____

We, _____, a reputed manufacturer/OEM of the products proposed under the above-mentioned RFP, having our registered office at _____ and development/manufacturing facilities at _____, hereby certify and confirm the following:

S. No.	Product Name as per RFP	Product Name as per OEM	Model	Version*
1				
2				

*Note – the proposed version is the latest available production version meeting bank's requirement as specified in the RFP.

1. We confirm that the products proposed above fully comply with the requirements specified in the RFP. The compliance against the Functional Requirement Specifications (FRS) and Technical Requirement Specifications (TRS) has been provided by us and submitted by the bidder in the prescribed format as part of the bid response.
2. We further confirm that our proposed products fully comply with the scope of work, technical specifications, service levels, interoperability requirements, support obligations, and all other applicable terms and conditions of the RFP relevant to the proposed solution.
3. We certify that the OEM make, model, and version declared herein are identical to those proposed by the bidder in the Undertaking, Technical Bid, and Masked BoM. No alternate product, model, version, equivalent offering, or substitute product has been proposed.
4. We confirm that all proposed product(s) are currently supported and commercially available and that no software, hardware, appliance, subscription, licence, or component proposed/supplied under this RFP shall reach End-of-Life (EOL) and/or End-of-Support (EOS) during the Contract Period.

5. We have attached the Software Bill of Materials (SBOM) and Cybersecurity Bill of Materials (CBOM - Public) for the proposed solution in the format prescribed under Annexure 20. The detailed/private SBOM and CBOM containing confidential or sensitive security information shall be provided to the Bank after issuance of the Purchase Order and execution of applicable confidentiality requirements.
6. We further confirm that we support secure, automated, and machine-readable exchange of SBOM/CBOM information through industry-recognized formats and mechanisms and shall facilitate the Bank in obtaining updated SBOM/CBOM information throughout the contract period.
7. We undertake to provide all necessary OEM support, software updates, security patches, vulnerability disclosures, technical advisories, and product lifecycle information for the duration of the contract.
8. We understand that any misrepresentation, incorrect declaration, or inconsistency between this declaration, the bidder's submission, the Undertaking, or the proposed products may result in rejection of the bid and/or any action deemed appropriate by the Bank.

For and on behalf of the OEM
Authorized Signatory: _____
Name: _____
Designation: _____
OEM Name: _____
Signature & Seal
Date: _____

16.19 Annexure 19: Stack Confirmation Sheet - Undertaking for Proposed OEM Products

(To be submitted on Bidder's Letterhead duly signed by the Authorized Signatory)

To,

General Manager (CISO)

STAFF TRAINING CENTRE PUNJAB AND SIND BANK

Punjab & Sind Bank, CISO cell 3rd Floor,

B-8/232, Naharpur Village Rd, Pocket 8, Sector 3B,

Rohini, Delhi, 110085

We hereby undertake that the products proposed under this bid are as detailed below. We further confirm that the details furnished herein are true and correct and shall exactly match the details provided in the Masked Bill of Materials (BoM) submitted as part of the bid.

In case of any discrepancy, inconsistency, omission, mismatch, or ambiguity between the Masked BoM and this Undertaking, the details provided in this Undertaking shall prevail for the purpose of technical evaluation and contract execution.

Solution:

S.No	Solution Name	Make of the Product	Model of the Product	**Version of the product**
1	SIEM			
2	SOAR			
3	UEBA			
4	Threat Intelligence Platform			
5	XDR			
6	Decoy/Honeypot			
7	Vulnerability assessment & Vulnerability Lifecycle management			
8	ITDR			
9	Application Security testing Tool			
10	Cloud Security Posture Management			
11	CNAPP			
12	CWPP			
13	CTEM			

Services:

S.No	Service Name	Make of the Service Provider
1	Breach Attack & Simulation	
2	Continuous Automated Red Teaming services	
3	Attack Surface management	
4	Phishing Simulation	
5	Digital risk management	

6	Dark web Monitoring	
7	Threat Intelligence Feed	
8	Threat Hunting services	

IT Infrastructure:

S.No	Component Name	Make of the Service Provider
1	Server	
2	Storage	
3	SAN Switch	
4	ToR Switch	
5	Racks	
6	…..	
7	…..	
8	…..	
9	…..	
10	…..	

1. We certify that all products proposed above are commercially available and supported by the respective OEMs.
2. We certify that the Make/OEM and Product Model mentioned above are identical to those quoted in the Masked BoM and shall be supplied in the event of award of contract.
3. We understand that the Bank shall evaluate the technical compliance based on the information furnished in this undertaking and supporting technical documents.
4. Any incorrect declaration, misrepresentation, substitution of OEM/model, or discrepancy between this undertaking and the submitted BoM may result in rejection of the bid and/or any other action deemed appropriate by the Bank.
5. The Bank reserves the right to seek OEM confirmation, product datasheets, licenses, authorizations, or any additional documentary evidence to validate the details furnished herein.
6. Proposing multiple options, alternate OEMs, substitute products, or equivalent solutions for any solution component is not permissible and may render the bid non-responsive and liable for rejection.

Authorized Signatory
Name: _____
Designation: _____
Bidder Name: _____
Signature & Seal: _____
Date: _____

16.20 Annexure 20: S-BOM & C-BOM DETAILS of all the proposed Tool/solutions

a. S-BOM

On OEM Letterhead

S.No.	Component	Component Name	Component Name	Component Name	Component Name	Component Name	Component Name
1.	Version						
2.	Description						
3.	Supplier						
4.	License						
5.	Originc						
6.	Dependencies						
7.	Vulnerabilities						
8.	Patch Status						
9.	Release Date						
10.	End of Life Date						
11.	Usage Restrictions						
12.	Checksums						
13.	Hashes						
14.	Executable Property						
15.	Archive Property						
16.	Structured Property						
17.	Unique Identifier						

b. C-BOM

On OEM Letterhead

S.No.	Component	Component Name	Component Name	Component Name	Component Name	Component Name	Component Name
1.	Version						
2.	Description						
3.	Supplier						
4.	License						
5.	Origin						
6.	Dependencies						
7.	Vulnerabilities						
8.	Patch Status						
9.	Release Date						
10.	End of Life Date						
11.	Usage Restrictions						
12.	Checksums						
13.	Hashes						
14.	Executable Property						
15.	Archive Property						
16.	Structured Property						
17.	Unique Identifier						

16.21Annexure 21: Sizing/Volumetrics, Data Retention and Current Infrastructure

Bidder based on their solution design and architecture may propose non production if required for testing, validation, upgrades, patching configuration changes, policy tuning, rule testing and other activities during the contract period without impacting production services.

The bidder shall ensure that all archived logs, records, events, alerts, forensic artefacts, audit trails, and other retained data can be restored and made available in the respective native technology platform and readable format whenever required by the Bank for forensic investigations, incident response, audit, compliance, regulatory, legal, or operational purposes.

The bidder shall be solely responsible for sizing all infrastructure components required for successful deployment and operation of the proposed solution, including but not limited to compute, storage, backup, network, bandwidth, IOPS, CPU, memory, servers, operating systems, databases, virtualization, cloud resources, and associated software. Such sizing shall be carried out in consultation with the respective infrastructure OEMs and solution/service OEMs and shall account for all performance, availability, retention, security, disaster recovery, and SLA requirements specified in the RFP.

The bidder and respective OEMs shall account for the projected growth, increase in transaction volumes, security events, log generation rates, storage consumption, user base, applications, and regulatory requirements throughout the contract period while arriving at the proposed sizing. The proposed solution shall meet all functional, technical, performance, scalability, availability, security, and service level requirements during the entire contract period. Any augmentation, upgrade, expansion, or replacement required due to inadequate sizing, incorrect assumptions, or failure to account for projected growth shall be carried out at no additional cost to the Bank inline with the terms stated in Section 7.13 - IT Infrastructure.

16.21.1 Current IT assets

S.No.	Current assets description	Current assets
	Centralized IT Infrastructure	
1	Servers deployed with OS, DB, Web/app component, middleware's, agents and other applications / software, private & public cloud setups, emerging technologies etc.	2500
2	Database	300
3	Intranet and internet facing business & non-business applications like CBS, Internet Banking, Mobile Banking, HRMS, O365 etc.	200
	Branches	
4	Desktops with various agents like AV, DLP, NAC, ITAM etc.	12000
5	Routers & Switches	7200

Note: The count of IT & Security Infra as listed above is tentative.

16.21.2 Volumetrics & Storage Solution-wise Requirements

Volumetrics

Solution Name	Day-1 Requirement	Scalability / Pro-Rata Requirement	Other Mandatory Requirements
Security Information and Event Management (SIEM)	Minimum 50,000 sustainable EPS / 3.24 TB/day, whichever is higher, at DC & DR.	Scalable up to 100,000 sustainable EPS / 6.48 TB/day, whichever is higher. Additional capacity in tranches of 10,000 EPS / 648 GB/day at quoted BOM rates.	All inline components shall operate in HA. Automatic failover within seconds without manual intervention. Each DC/DR environment shall be independently provisioned for full peak load. Average Event Size: 750 Bytes/Event.
Security Orchestration, Automation & Response (SOAR)	Minimum 5 concurrent users/analysts.	Additional users/licenses shall be available on pro-rata basis as per BOM.	No limitation on SOAR licenses based on number of events, playbooks or actions.
User & Entity Behaviour Analytics (UEBA)	Minimum 50,000 sustainable EPS / 3.24 TB/day, whichever is higher, at DC & DR; 12,000 endpoint users.	Scalable up to 100,000 sustainable EPS / 6.48 TB/day, whichever is higher and 16,000 endpoint users. Additional capacity in tranches of 500 endpoints at quoted BOM rates.	

Solution Name	Day-1 Requirement	Scalability / Pro-Rata Requirement	Other Mandatory Requirements
Deception Technology (Decoy/Honeypot)	Complete Decoy/Deception solution covering a minimum of 15 applications/networks/devices across 50 segments, spanning DC and DR. A minimum of 15 decoys shall be created/deployed.	Additional decoy connectors/components shall be supported through customization as required. Scalability Complete Decoy/Deception solution covering a minimum of 200 applications/networks/devices across 50 segments, spanning DC and DR. A minimum of 15 decoys shall be created/deployed. Additional capacity in tranches of 5 Decoy at quoted BOM rates.	
Extended Detection & Response (XDR)	• Minimum 12,000 users/endpoints. • Minimum 10 Gbps throughput, To provide comprehensive visibility across key network aggregation points	Scalable up to 16,000 users/endpoints. Additional capacity in tranches of 500 endpoints at quoted BOM rates.	
Threat Intelligence Platform (TIP)	Minimum 5 user licenses.	Additional users/licenses shall be available on pro-rata BOM basis.	

Solution Name	Day-1 Requirement	Scalability / Pro-Rata Requirement	Other Mandatory Requirements
Vulnerability Assessment (VA) & Vulnerability Lifecycle Management (VLM)	Minimum 4,000 IPs.	Scalable beyond Day-1 capacity on pro-rata BOM basis.	Required scanners/engines/components shall support the specified deployment architecture.
Identity Threat Detection & Response (ITDR)	Minimum 12,000 users/endpoints.	Scalable up to 16,000 users/endpoints. Additional capacity in tranches of 500 endpoints at quoted BOM rates.	
Application Security Testing (AST)	SAST: 1 Enterprise license, unlimited applications and unlimited scans/LOC analysed, with 30 users. DAST: 1 Enterprise license covering minimum 25 web-facing applications.	Additional applications/users/capacity shall be available on pro-rata BOM basis.	No restriction on number of users who can log in/view the console.
Cloud Security Posture Management (CSPM)	Minimum 20 VMs	Scalable beyond Day-1 capacity on pro-rata BOM basis.	
Cloud-Native Application Protection Platform (CNAPP)	Minimum 20 VPCs/VNets and 100 VMs.	Scalable beyond Day-1 capacity on pro-rata BOM basis.	
Cloud Workload Protection Platform (CWPP)	Minimum 20 VPCs/VNets and 100 VMs.	Scalable beyond Day-1 capacity on pro-rata BOM basis.	

Solution Name	Day-1 Requirement	Scalability / Pro-Rata Requirement	Other Mandatory Requirements
Continuous Threat Exposure Management (CTEM)	Unlimited Vulnerability/Exposure Findings and Attack Paths/Exposure Relationships; 12,000 users/endpoints; 4,000 IPs.	Scalable up to 16,000 users/endpoints and beyond Day-1 IP capacity on pro-rata BOM basis.	No limitation on vulnerabilities, exposures, attack paths, risk relationships, remediation records or findings discovered, correlated, prioritised, validated or retained.

All data ingress and egress associated with the Solution shall be provided at no additional cost to the Bank. This shall include, without limitation, all data transfer and network-related activities associated with log/data ingestion, API traffic, system integrations, backup, replication, archival, restoration, data retrieval, data export, migration, and exit/transition activities.

The Bidder shall ensure that its quoted price is all-inclusive and shall incorporate all applicable charges levied by the Cloud Service Provider(s), including data-transfer and data-retrieval charges, inter-region and inter-zone transfer charges, API-related charges, and any other associated network or data-movement charges arising in connection with the Solution.

Under no circumstances shall the Bidder levy any additional or separate charges on the Bank for such data ingress, egress, transfer, retrieval, or associated network activities during the entire contractual period, including implementation, operations, backup/disaster recovery, migration, and exit/transition.

The Bidder shall be solely responsible for identifying, estimating, and including all such applicable charges in its commercial proposal for the duration of the contract.

The Bank will procure additional licenses, services, hardware as per the rate provided in the respective Sheets or on pro-rata basis.

Solutions	Components		Requirements	Period	Details
SIEM	Raw Log Storage On Cloud/On-premise primary storage	Raw logs shall be retained in their original/unmodified form, including timestamp, source and relevant metadata.	Minimum 3 Month	1. Logs shall be searchable/retrievable. 2. No alteration/deletion before expiry of retention period without Bank approval. 3. Storage shall support required ingestion and peak load.	

Solutions	Components		Requirements	Period	Details
	Processed Log Storage on Cloud	Parsed, normalized, enriched, indexed and correlated logs, including associated metadata and context, shall be retained.	Hot Storage – 12 Months: The most recent 12 months of processed logs shall be maintained in Hot Storage and shall be immediately searchable and retrievable through the SIEM without requiring restoration, rehydration or recall from archival storage. Warm Storage – 48 Months: The subsequent 48 months of processed logs shall be maintained in Warm Storage and shall remain searchable and retrievable with minimum latency to support historical investigation, threat hunting, compliance and forensic requirements.	1. Logs shall remain searchable and retrievable. 2. Adequate storage shall be provisioned for indexing, enrichment and growth. 3. Historical investigation shall be supported.	
	Backup	SIEM SaaS application specific configurations, including but not limited to policies, correlation rules, detection rules, dashboards, workflows, user/role configurations and other application-specific configurations, shall be backed up by the Bidder/OEM on Cloud/CSP infrastructure.	As backup & retention Policy	1. Backup shall be protected against unauthorized access, modification and deletion. 2. Data transferred to LTS shall remain retrievable and restorable throughout the retention period. 3. Bidder shall provide all required backup agents, APIs, connectors, utilities and data-transfer mechanisms. 4. Restoration shall meet specified RTO/RPO. 5. Backup and restoration testing shall be conducted quarterly.	

Solutions	Components		Requirements	Period	Details
		Bank-owned SIEM data shall be backed up to Bank-designated DC & DR Backup. This shall include Raw Logs, Parsed/Normalized/Correlated Logs, security data, metadata, reports and other Bank-owned information. The respective application shall generate and maintain comprehensive audit trails, including relevant user and system activities, and shall make such audit trails available to the Bank. The audit trails shall be backed up and archived on the Bank's infrastructure (i.e., Long-Term Storage)		6. No additional license, software, transfer, retrieval or restoration charges shall apply	
SOAR	Primary Data Storage on cloud	SOAR incidents, cases, playbooks, execution logs, alerts, investigation data, audit trails, metadata and other Bank-owned security information shall be retained on Cloud/CSP infrastructure.	Minimum 3 Months	• Data shall remain searchable and retrievable. • Historical investigation shall be supported. • Adequate storage for data growth shall be provisioned.	
	Backup	On-Cloud Application-specific configuration, not limited to, shall be backed up by Bidder/OEM on Cloud/CSP infrastructure.	As backup & retention Policy		

Solutions	Components		Requirements	Period	Details
		ON-premise Raw & Normalised/parsed/Enriched logs, data only shall be backed up to Bank-designated DC & DR Backup. This includes logs, events, alerts, incidents, findings, telemetry, reports, metadata and other Bank-owned information The respective application shall generate and maintain comprehensive audit trails, including relevant user and system activities, and shall make such audit trails available to the Bank. The audit trails shall be backed up and archived on the Bank's infrastructure (i.e., Long-Term Storage)			
UEBA	Primary Data Storage on cloud	User/entity activity data, behavioural analytics, risk scores, anomalies, alerts, investigation data, metadata and other security information shall be retained on Cloud/CSP infrastructure.	Minimum 3 Months	• Searchable and retrievable.• Historical investigation and behavioural analysis shall be supported.• Adequate storage for growth shall be provisioned.	
	Backup	On-Cloud: UEBA application-specific configurations, policies, detection models/rules, dashboards, workflows and	As backup & retention Policy	• Secure backup.• Required backup/data-transfer utilities included.• Restoration as per RTO/RPO.• Quarterly testing.• No additional charges.	

Solutions	Components		Requirements	Period	Details
		user/role configurations shall be backed up by Bidder/OEM on Cloud/CSP infrastructure. Bank: Bank-owned events, alerts, behavioural data, risk information, findings, reports and other Bank-owned information shall be backed up to Bank-designated DC & DR Backup. This includes logs, events, alerts, incidents, findings, telemetry, reports, metadata and other Bank-owned information The respective application shall generate and maintain comprehensive audit trails, including relevant user and system activities, and shall make such audit trails available to the Bank. The audit trails shall be backed up and archived on the Bank's infrastructure (i.e., Long-Term Storage)			
XDR	Primary Data Storage on cloud	XDR telemetry, alerts, incidents, investigation data, endpoint/network/cloud security data, detection results, metadata and related security	Minimum 3 Months	• Searchable and retrievable.• Historical investigation shall be supported.• Storage shall account for ingestion and growth.	

Solutions	Components		Requirements	Period	Details
		information shall be retained on Cloud/CSP infrastructure.			
	Backup	On-Cloud: XDR policies, detection rules, configurations, dashboards, workflows and user/role configurations shall be backed up on Cloud/CSP. On-premise: Logs, telemetry, alerts, incidents, investigation data and reports shall be backed up to Bank DC and DR, as applicable. This includes logs, events, alerts, incidents, findings, telemetry, reports, metadata and other Bank-owned information The respective application shall generate and maintain comprehensive audit trails, including relevant user and system activities, and shall make such audit trails available to the Bank. The audit trails shall be backed up and archived on the Bank's infrastructure (i.e., Long-Term Storage)	As backup & retention Policy	• Secure backup.• Required connectors/APIs/utilities included.• Restoration as per RTO/RPO.• Quarterly restoration testing.• No additional charges.	
TIP	Primary Data	Threat Intelligence data, IoCs, threat actors, campaigns,	Minimum 3 Months	• Intelligence shall remain searchable and retrievable.• Historical intelligence shall be available for	

Solutions	Components		Requirements	Period	Details
	Storage on cloud	relationships, enrichment, sightings, investigations, metadata and associated intelligence shall be retained on Cloud/CSP infrastructure.		investigation.• Adequate storage for intelligence growth shall be provisioned.	
	Backup	TIP configurations, feeds, policies, workflows, integrations and user/role configurations shall be backed up on Cloud/CSP. Bank-owned intelligence, IoCs, enrichment, reports and other Bank-generated data shall be backed up to Bank DC/DR/LTS, as applicable. This includes logs, events, alerts, incidents, findings, telemetry, reports, metadata and other Bank-owned information The respective application shall generate and maintain comprehensive audit trails, including relevant user and system activities, and shall make such audit trails available to the Bank. The audit trails shall be backed up and archived on the Bank's infrastructure (i.e., Long-Term Storage)	As backup & retention Policy	• Data shall be exportable in open/readable format.• Secure backup and restoration.• Required APIs/connectors included.• Quarterly testing.• No additional charges.	

Solutions	Components		Requirements	Period	Details
CSPM	Primary Data Storage on cloud	Cloud asset inventory, configuration data, compliance findings, misconfigurations, alerts, risk information, assessment history and associated metadata shall be retained on Cloud/CSP infrastructure.	Minimum 3 Months	• Historical findings shall be searchable and retrievable.• Adequate storage for asset and finding growth.	
	Backup	CSPM policies, rules, configurations, dashboards, workflows and user/role configurations shall be backed up on Cloud/CSP. Bank-owned findings, reports, assessment data and other security information shall be backed up to Bank DC/DR/LTS, as applicable. This includes logs, events, alerts, incidents, findings, telemetry, reports, metadata and other Bank-owned information The respective application shall generate and maintain comprehensive audit trails, including relevant user and system activities, and shall make such audit trails available to the Bank. The audit trails shall be backed up and archived on the Bank's	As backup & retention Policy	• Secure backup.• Restoration as per RTO/RPO.• Required utilities included.• Quarterly testing.• No additional charges.	

Solutions	Components		Requirements	Period	Details
		infrastructure (i.e., Long-Term Storage)			
CNAPP	Primary Data Storage on cloud	CNAPP findings, cloud asset/workload information, posture data, vulnerabilities, risks, alerts, configuration data, metadata and investigation information shall be retained on Cloud/CSP infrastructure.	Minimum 3 Months	• Searchable and retrievable.• Historical investigation supported.• Adequate storage for growth.	
	Backup	CNAPP policies, configurations, detection rules, dashboards, workflows and user/role configurations shall be backed up on Cloud/CSP. Bank-owned findings, reports, security data and assessment information shall be backed up to Bank DC/DR/LTS, as applicable. This includes logs, events, alerts, incidents, findings, telemetry, reports, metadata and other Bank-owned information The respective application shall generate and maintain comprehensive audit trails, including relevant user and system activities, and shall make such audit trails available to the Bank. The audit trails	As backup & retention Policy	• Secure backup.• Required APIs/connectors included.• Restoration as per RTO/RPO.• Quarterly testing.• No additional charges.	

Solutions	Components		Requirements	Period	Details
		shall be backed up and archived on the Bank's infrastructure (i.e., Long-Term Storage)			
CWPP	Primary Data Storage on cloud	Workload telemetry, security events, vulnerabilities, alerts, incidents, workload inventory, investigation data and associated metadata shall be retained on Cloud/CSP infrastructure.	Minimum 3 Months	• Searchable and retrievable.• Historical investigation supported.• Storage shall account for workload growth.	
	Backup	CWPP policies, configurations, rules, dashboards, workflows and user/role configurations shall be backed up on Cloud/CSP. Bank-owned workload security data, alerts, findings, reports and other security information shall be backed up to Bank DC/DR/LTS, as applicable. This includes logs, events, alerts, incidents, findings, telemetry, reports, metadata and other Bank-owned information The respective application shall generate and maintain comprehensive audit trails, including relevant user and system activities, and shall make such audit trails available to the Bank. The audit trails	As backup & retention Policy	• Secure backup.• Restoration as per RTO/RPO.• Required utilities included.• Quarterly testing.• No additional charges.	

Solutions	Components		Requirements	Period	Details
		shall be backed up and archived on the Bank's infrastructure (i.e., Long-Term Storage)			
CTEM	Primary Data Storage on cloud	Exposure findings, vulnerabilities, attack-path information, asset information, risk/prioritization data, validation results, remediation status and associated metadata shall be retained on Cloud/CSP infrastructure.	Minimum 3 Months	• Historical exposure information shall be searchable and retrievable.• Historical assessment and remediation tracking shall be supported.	
	Backup	CTEM configurations, policies, assessment settings, workflows, dashboards and user/role configurations shall be backed up on Cloud/CSP. Bank-owned exposure findings, assessment results, reports and other security information shall be backed up to Bank DC/DR/LTS, as applicable. This includes logs, events, alerts, incidents, findings, telemetry, reports, metadata and other Bank-owned information The respective application shall generate and maintain comprehensive audit trails, including relevant user and system activities, and shall make such audit trails available	As backup & retention Policy	• Secure backup.• Required APIs/connectors/utilities included.• Restoration as per RTO/RPO.• Quarterly testing.• No additional charges.	

Solutions	Components		Requirements	Period	Details
		to the Bank. The audit trails shall be backed up and archived on the Bank's infrastructure (i.e., Long-Term Storage)			
Deception	Primary Data Storage on cloud /On-premise	SaaS + On-Premise: Deception events, alerts, incidents, telemetry, investigation data, decoy activity, metadata and other Bank-owned security information shall be retained on Cloud/CSP infrastructure. Fully On-Premise: Solution data shall be retained within the Bank's designated infrastructure.	Minimum 3 Months	• Data shall remain searchable and retrievable. • Historical investigation shall be supported. • Adequate storage shall be provisioned.	
	Backup	Option 1: SaaS + On-Premise: a) On-cloud: Application-specific configurations shall be backed up by Bidder/OEM on Cloud/CSP infrastructure. b) On-premise: Bank-owned deception logs, events, alerts, telemetry, findings, reports and other Bank-owned data shall be backed up to Bank DC & DR Backup. This includes logs, events, alerts, incidents, findings, telemetry, reports, metadata	As backup & retention Policy	• Secure backup. • Restoration as per RTO/RPO. • No additional charges.	

Solutions	Components		Requirements	Period	Details
		and other Bank-owned information The respective application shall generate and maintain comprehensive audit trails, including relevant user and system activities, and shall make such audit trails available to the Bank. The audit trails shall be backed up and archived on the Bank's infrastructure (i.e., Long-Term Storage) Option 2: Fully On-Premise: Full solution backup shall be maintained on Bank-designated DC & DR Backup. The respective application shall generate and maintain comprehensive audit trails, including relevant user and system activities, and shall make such audit trails available to the Bank. The audit trails shall be backed up and archived on the Bank's infrastructure (i.e., Long-Term Storage)			
VA & VLM	Primary Data Storage on cloud /On-premise	SaaS + On-Premise: Vulnerability scan results, asset inventory, vulnerability findings, risk scores, remediation status, assessment	Minimum 3 Months	• Data shall remain searchable and retrievable. • Historical vulnerability assessment and remediation tracking shall be supported. • Adequate storage shall be provisioned for asset, scan and vulnerability data growth	

Solutions	Components		Requirements	Period	Details
		history, reports, metadata and other Bank-owned security information shall be retained on Cloud/CSP infrastructure. Fully On-Premise: Solution data, including scan results, asset inventory, vulnerability findings, risk information, remediation status, reports, metadata and other relevant data, shall be retained within the Bank's designated infrastructure.			
	Backup	Option 1: SaaS + On-Premise: a) On-Cloud: Application-specific configurations, including policies, scan configurations, assessment settings, dashboards, workflows, user/role configurations and other application-specific configurations, shall be backed up by Bidder/OEM on Cloud/CSP infrastructure. b) On-Premise: Bank-owned vulnerability data, including scan results, asset inventory, vulnerability findings, risk information, remediation status, reports, metadata and other Bank-owned data shall	As backup & retention Policy	• Secure backup against unauthorized access, modification and deletion. • Restoration/retrieval shall meet specified RTO/RPO. • Required backup agents, connectors, APIs and utilities shall be provided. • No additional license/software/backup/restoration charges.	

Solutions	Components		Requirements	Period	Details
		be backed up to Bank DC & DR Backup. The respective application shall generate and maintain comprehensive audit trails, including relevant user and system activities, and shall make such audit trails available to the Bank. The audit trails shall be backed up and archived on the Bank's infrastructure (i.e., Long-Term Storage) Option 2: Fully On-Premise: Full solution backup, including application/configuration, databases, scan results, asset inventory, vulnerability findings, reports, metadata and other relevant solution data, shall be maintained on Bank-designated DC & DR Backup. The respective application shall generate and maintain comprehensive audit trails, including relevant user and system activities, and shall make such audit trails available to the Bank. The audit trails shall be backed up and archived on the Bank's infrastructure (i.e., Long-Term Storage)			

Solutions	Components		Requirements	Period	Details
ITDR	Primary Data Storage on cloud /On-premise	SaaS + On-Premise: Identity telemetry, authentication events, identity-related alerts, incidents, risk/anomaly data, detection results, investigation data, metadata and other Bank-owned security information shall be retained on Cloud/CSP infrastructure. Fully On-Premise: Solution data, including identity telemetry, authentication events, alerts, incidents, risk/anomaly data, detection results, investigation data, metadata and other relevant data, shall be retained within the Bank's designated infrastructure.	Minimum 3 Months	• Data shall remain searchable and retrievable. • Historical identity-threat investigation shall be supported. • Adequate storage shall be provisioned for data growth.	
	Backup	Option 1: SaaS + On-Premise: a) On-Cloud: Application-specific configurations, including policies, detection rules, dashboards, workflows, user/role configurations, integration settings and other application-specific configurations, shall be backed up by Bidder/OEM on Cloud/CSP infrastructure. b) On-Premise: Bank-owned identity telemetry, authentication events, alerts,	As backup & retention Policy	• Secure backup against unauthorized access, modification and deletion. • Restoration/retrieval shall meet specified RTO/RPO. • Required backup agents, connectors, APIs and utilities shall be provided. • No additional license/software/backup/restoration charges.	

Solutions	Components		Requirements	Period	Details
		incidents, findings, investigation data, reports, metadata and other Bank-owned data shall be backed up to Bank DC & DR Backup. The respective application shall generate and maintain comprehensive audit trails, including relevant user and system activities, and shall make such audit trails available to the Bank. The audit trails shall be backed up and archived on the Bank's infrastructure (i.e., Long-Term Storage) Option 2: Fully On-Premise:Full solution backup, including application/configuration, databases, identity telemetry, events, alerts, findings, reports, metadata and other relevant solution data, shall be maintained on Bank-designated DC & DR Backup. The respective application shall generate and maintain comprehensive audit trails, including relevant user and system activities, and shall make such audit trails available to the Bank. The audit trails shall be backed up and archived			

Solutions	Components		Requirements	Period	Details
		on the Bank's infrastructure (i.e., Long-Term Storage)			

Note: During the Contract Period, the Bank may, at its sole discretion and based on its business, operational, security or capacity requirements, procure additional capacity, licenses, subscriptions, appliances, resources or other components from the successful Bidder. Any such additional procurement shall be made on a **pro-rata basis with reference to the unit rates quoted and accepted under the original commercial bid**

16.21.3 Deployment and Data Retention

The Bidder shall ensure that the proposed Primary Storage, Backup Storage / Backup Appliance and Long-Term Storage (LTS) are adequately sized to meet the Bank's data retention, backup, recovery, archival and operational requirements for the entire contract period.
All storage sizing and capacity calculations shall, at a minimum, consider databases, indexes, metadata, replication, snapshots, High Availability (HA) / Disaster Recovery (DR) overhead, backup copies, projected data growth, temporary/staging storage, system and infrastructure overhead, and adequate operational headroom.

Retention Requirement:

Backup Type	Retention Location	Retention Period
On- Premise		
Daily Incremental Backup	Backup Storage / Backup Appliance	2 Weeks
Weekly Full Backup	Backup Storage / Backup Appliance	2 Weeks
Weekly Full backup	Long-Term Storage (LTS)	Entire Duration of the Contract
On- Cloud Raw/Normalized logs, data, information's etc. generated/utilized by any cloud-based solution shall be transferred to the on-premise infrastructure on a near-real-time basis and archived on Long-Term Storage by EOD. The bidder shall provision adequate on-premise backup storage capacity to retain at least 7 days of logs to cater for any transfer or system failure. Daily incremental backups shall be maintained on dedicated long terms storage for the duration of the contract.		
Backup & LTS Transfer	The Bidder shall provide all required agents, connectors, APIs, interfaces, utilities and	Throughout Contract	No additional license, software, transfer, migration or restoration charges shall apply.

Backup Type	Retention Location		Retention Period
	mechanisms required to perform backup and transfer/migration of applicable data to the Bank's Backup Storage and LTS infrastructure.		
Restoration	Backup and LTS data shall be capable of restoration/retrieval whenever required by the Bank.	Throughout Contract	Restoration shall meet the RTO/RPO specified in the RFP.
LTS	All backups, logs, security data, configurations, reports, metadata and other Bank-owned information requiring long-term retention shall be stored on the Bank's designated on-premises LTS infrastructure.	Entire Contract Period	1. Secure transfer to LTS from backup storage/appliance. 2. Data shall remain retrievable/restorable throughout retention period. 3. Restoration shall meet specified RTO/RPO. 4. Required connectors/APIs/utilities shall be provided by Bidder. 5. No additional license, transfer or restoration charges.
Archived Log Retrieval, Restoration and Testing **The solution shall support secure long-term retention, retrieval and restoration of archived logs in accordance with the Bank's defined retention policies. Logs transferred to Long-Term Storage (LTS) shall remain available for retrieval throughout the applicable retention period.** **The solution shall provide the capability to:**			

Backup Type	Retention Location	Retention Period
1) Retrieve selected archived logs on demand from Long-Term Storage (LTS) based on defined time periods, source, event attributes, search criteria or other relevant parameters. **2) Restore retrieved archived logs from LTS either to the original SIEM/platform, wherever technically supported, or to a bidder proposed application,** **3) Retrieved archived logs from LTS shall be capable of being restored on to Bidder/OEM-proposed ETL application where the restored logs can be accessed, searched, and tested for integrity, completeness, readability, original timestamps, source information and relevant metadata. The Bidder/OEM shall propose and provide the required application, tools, utilities and mechanisms for such restoration and testing.** **4) Support at least quarterly restoration testing of archived logs from LTS, using representative archived data, to validate successful retrieval, restoration, integrity, completeness and readability of the archived logs.** **5) Provide restoration test reports upon request, including the test period/data set, volume of data restored, restoration status, integrity/validation results and any exceptions observed.** **6) Ensure that retrieval or restoration activities do not alter, overwrite, delete or compromise the integrity of the original archived logs maintained in LTS.** **The Bidder/OEM shall provide all required software, agents, APIs, connectors, utilities and mechanisms necessary for retrieval, restoration and transfer of archived logs to the designated Bank environment. The retrieval, restoration and testing capabilities shall remain available throughout the applicable retention period and shall be provided without any additional license, retrieval, data-transfer or restoration charges.** **Any on-premises infrastructure, including for successful restoration testing, required for delivery, integration, operation or support shall be proposed, supplied, deployed, configured and maintained by the Bidder as part of the solution.** **The Bidder shall clearly specify the required compute, storage, network, security, connectors, appliances and other infrastructure components in the BOM.** **1) Long-Term Storage (LTS) shall be deployed at the Bank's designated NDC and NDR locations.** **2) Applicable backups shall be transferred/migrated to LTS as per the Bank's Backup & Retention Policy and retained for the required contract period.** **3) Restoration testing shall be performed from both DC and DR as per the Bank's defined schedule.**		

Backup Type	Retention Location	Retention Period
4) The Bidder shall provide all required licenses, software, agents, connectors, APIs, utilities and technical support for backup, transfer, restoration and testing. **5) No additional charges shall be payable for the above activities.** **6) Bank can access, search and validate restored logs**		

Note: Upon completion of the two (2) month retention period on the Backup Storage, the applicable Monthly Full Backups shall be migrated to Long-Term Storage (LTS) at bank's DC & DR and retained for the entire duration of the contract.

The Bidder shall provide and deploy the proposed Backup Solution, Backup Storage / Backup Appliance and Long-Term Storage (LTS) at both the Bank's designated Primary Data Centre (DC) and Disaster Recovery Centre (DR).

The Bidder shall provide the required backup infrastructure, storage capacity, software, licenses, management components, agents, connectors, replication mechanisms and other components necessary for complete operation of the Backup and LTS solution at both locations.
The Bidder shall ensure that failure or unavailability of one site does not result in loss of the backup or archived data required to meet the applicable retention requirements.

The proposed architecture shall ensure that backup and archived data stored at DC and DR remains protected against unauthorized access, modification, corruption and deletion

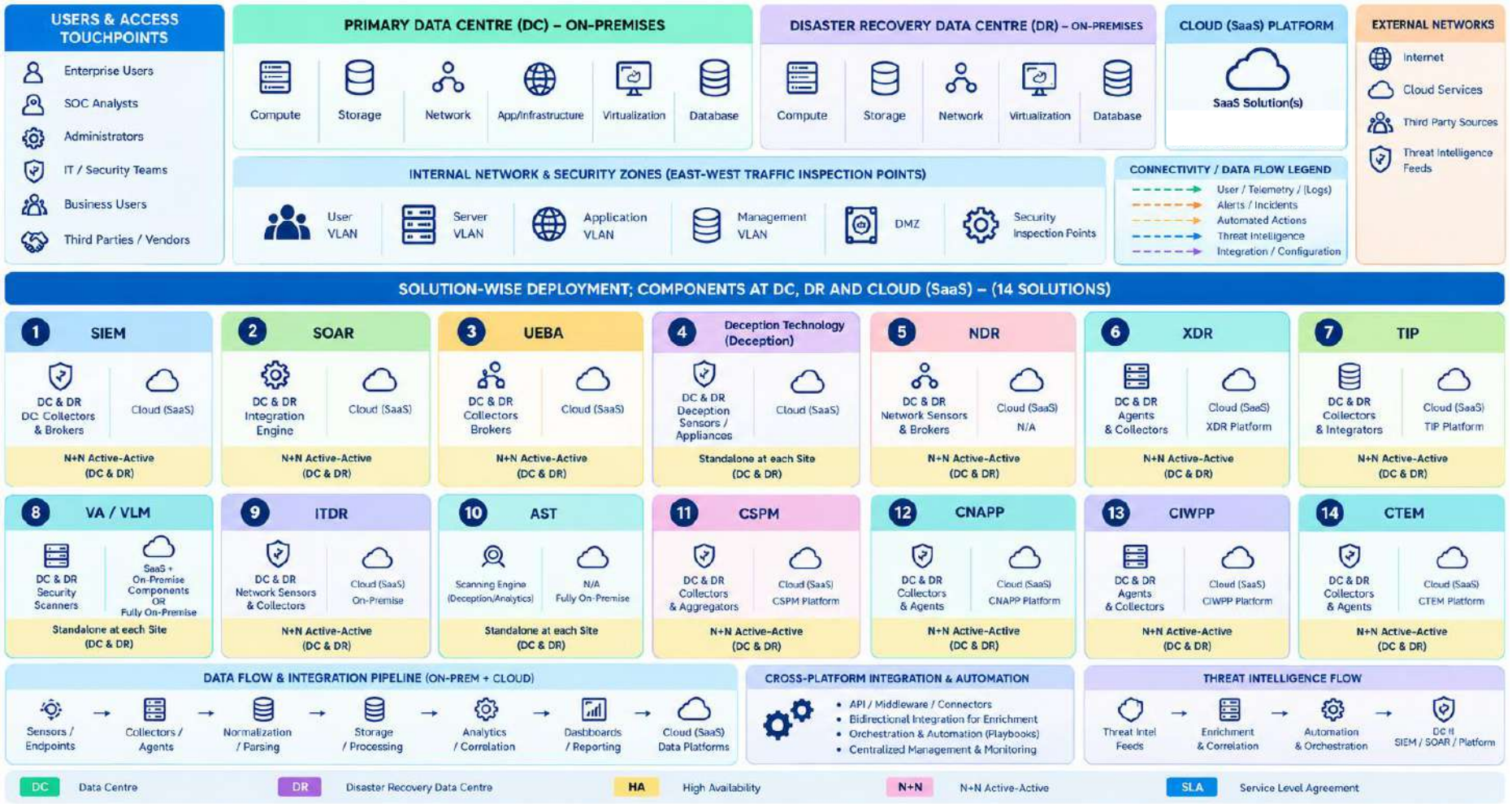
The proposed Backup and Retrieval Solution at bank's DC & DR shall be sized to support the complete backup and retention policy specified above. The sizing shall consider the actual backup data volume, expected daily change rate, deduplication and/or compression efficiency (where applicable), backup metadata, replication, redundancy, storage overhead, growth projections, and sufficient operational headroom.

The bidder shall ensure that all backed up and archived data, including logs, configurations, reports, videos, databases, indexes, metadata, and other associated artefacts, remain recoverable, readable, and accessible throughout the applicable retention period.

The solution shall maintain data integrity and availability throughout the retention lifecycle and shall ensure that backup, archival, restoration, retrieval, and forensic activities do not adversely impact production operations or applicable regulatory and compliance requirements.

The proposed Primary, backup storage and long-term storage (LTS) shall be adequately sized not only to meet the prescribed backup and retention requirements but also to support data restoration, retrieval, search, and forensic investigation activities. The bidder shall ensure that all backed up and archived data, logs, configurations, reports, videos, and other artefacts remain recoverable, readable, and accessible throughout the applicable retention period without impacting operational or regulatory requirements.

16.21.4 Solutions & Services – Master Deployment Matrix



A. Solutions

#	Solution	Permitted Deployment Model	Bank-Site / On-Premises Components	HA / DR Requirement
1	Security Information and Event Management (SIEM)	SaaS + On-Premises Components	The bidder shall provide, deploy, configure and support all Bank-site components required under the proposed OEM architecture, including Log Collectors, Brokers, Aggregators or equivalent components.	Bank-site components shall be deployed in N+N Active-Active configuration at both DC and DR. The SaaS service shall comply with the prescribed uptime SLA. The Management Console shall be accessible from both DC and DR.
2	Security Orchestration, Automation & Response (SOAR)	SaaS + On-Premise Components	The bidder shall provide, deploy, configure and support all Bank-site components required for integration, orchestration, enforcement and execution of actions, including Integration, Enforcement or equivalent components.	Bank-site components shall be deployed in N+N Active-Active configuration at both DC and DR. The SaaS service shall comply with the prescribed uptime SLA. The Management Console shall be accessible from both DC and DR.
3	User & Entity Behaviour Analytics (UEBA)	SaaS + On-Premise Components	The bidder shall provide, deploy, configure and support all Bank-site components required for data collection and ingestion, including Collectors, Brokers or equivalent components.	Bank-site components shall be deployed in N+N Active-Active configuration at both DC and DR. The SaaS service shall comply with the prescribed uptime SLA. The Management Console shall be accessible from both DC and DR.

#	Solution	Permitted Deployment Model	Bank-Site / On-Premises Components	HA / DR Requirement
4	Deception Technology (Decoy/Honeypot)	SaaS + On-Premise Components OR Fully On-Premise	**SaaS + On-Premise model:** The bidder shall provide, deploy, configure and support all Bank-site components required under the proposed OEM architecture, including Deceptors, Sensors, Agents, Enforcers or equivalent components. OR **Fully On-Premises:** The bidder shall provide, deploy, configure and support all solution components required for complete functionality within the Bank's designated infrastructure.	**SaaS + On-Premise:** Bank-site components shall be deployed at both DC and DR in Standalone mode. The SaaS service shall comply with the prescribed uptime SLA OR **Fully On-Premises:** The complete solution shall be deployed at both DC and DR in Standalone mode. The Management Console shall be accessible from both DC and DR.
5	Extended Detection & Response (XDR)	SaaS + On-Premise Components	The bidder shall provide, deploy, configure and support all Bank-site components required under the proposed OEM architecture, including Agents, Brokers, Collectors, Enforcers or equivalent components. The bidder shall provide, deploy, configure and support all solution components required for complete functionality	Bank-site components shall be deployed in N+N Active-Active configuration at both DC and DR. The SaaS service shall comply with the prescribed uptime SLA. The Management Console shall be accessible from both DC and DR.

#	Solution	Permitted Deployment Model	Bank-Site / On-Premises Components	HA / DR Requirement
6	Threat Intelligence Platform (TIP)	SaaS + On-Premise Components	The bidder shall provide, deploy, configure and support all Bank-site components required for integration with Bank systems, including Collectors, Integrators, Connectors or equivalent components.	Bank-site components shall be deployed in N+N Active-Active configuration at both DC and DR. The SaaS service shall comply with the prescribed uptime SLA. The Management Console shall be accessible from both DC and DR.
7	Vulnerability Assessment (VA) & Vulnerability Lifecycle Management (VLM)	SaaS + On-Premise Components OR **Fully On-premise**	**SaaS + On-Premise:** The bidder shall provide, deploy, configure and support all Bank-site components required under the proposed OEM architecture, including Sensors, Collectors, Scanner, Enforcers or equivalent components. OR **Fully On-Premise:** The bidder shall provide, deploy, configure and support all solution components required for complete functionality within the Bank's designated infrastructure.	**SaaS + On-Premise components:** All required **Bank-site component**s shall be deployed in standalone configuration at both DC and DR. The SaaS service shall comply with the prescribed uptime SLA requirements. **OR** **Fully On-Premise:** The complete solution shall be deployed in standalone configuration at both DC and DR. The Standalone management Console shall be accessible from both DC and DR.

#	Solution	Permitted Deployment Model	Bank-Site / On-Premises Components	HA / DR Requirement
8	Identity Threat Detection & Response (ITDR)	SaaS + On-Premise Components OR Fully On-Premise	**SaaS + On-Premise:** The bidder shall provide, deploy, configure and support all Bank-site components required under the proposed OEM architecture, including Network Sensors, Collectors, Brokers, Enforcers or equivalent components. OR **Fully On-Premise:** The bidder shall provide, deploy, configure and support all solution components required for complete functionality within the Bank's designated infrastructure.	**SaaS + On-Premise components:** All required **Bank-site component**s shall be deployed in N+N Active-Active configuration at both DC and DR. The SaaS service shall comply with the prescribed uptime SLA requirements. **OR** **Fully On-Premise:** The complete solution shall be deployed in N+N Active-Active configuration at both DC and DR. The Standalone management Console shall be accessible from both DC and DR.
9	Application Security Testing (AST)	Fully On-Premise	The bidder shall provide, deploy, configure and support all solution components required for complete functionality, including AST Management Server, Scanners, Controllers and other necessary components, within the Bank's designated infrastructure.	The solution shall be deployed at both DC and DR. Standalone deployment at each site shall be acceptable unless HA is required/supported by the proposed OEM architecture. The Management Console shall be accessible from both DC and DR.
10	Cloud Security Posture Management (CSPM)	SaaS + On-Premise Components	The bidder shall provide, deploy, configure and support all Bank-site components required under the proposed OEM architecture for integration with the Bank's cloud and other systems, including Collectors, Integrators, Connectors or equivalent components.	All required Bank-site components shall be deployed in N+N Active-Active configuration at both DC and DR. The SaaS service shall comply with the prescribed uptime SLA. The Management Console shall be accessible from both DC and DR.

#	Solution	Permitted Deployment Model	Bank-Site / On-Premises Components	HA / DR Requirement
11	Cloud-Native Application Protection Platform (CNAPP)	SaaS + On-Premise Components	The bidder shall provide, deploy, configure and support all Bank-site components required under the proposed OEM architecture for protection and integration of the Bank's cloud-native applications, including Collectors, Integrators, Connectors, Agents or equivalent components.	All required Bank-site components shall be deployed in N+N Active-Active configuration at both DC and DR. The SaaS service shall comply with the prescribed uptime SLA. The Management Console shall be accessible from both DC and DR.
12	Cloud Workload Protection Platform (CWPP)	SaaS + On-Premise Components	The bidder shall provide, deploy, configure and support all Bank-site components required under the proposed OEM architecture for protection and monitoring of the Bank's cloud workloads, including Agents, Sensors, Collectors, Connectors or equivalent components.	All required Bank-site components shall be deployed in N+N Active-Active configuration at both DC and DR. The SaaS service shall comply with the prescribed uptime SLA. The Management Console shall be accessible from both DC and DR.
13	Continuous Threat Exposure Management (CTEM)	SaaS + On-Premise Components	The bidder shall provide, deploy, configure and support all Bank-site components required under the proposed OEM architecture, including Collectors, Scanners, Integrators, Connectors or equivalent components.	All required Bank-site components shall be deployed in N+N Active-Active configuration at both DC and DR. The SaaS service shall comply with the prescribed uptime SLA. The Management Console shall be accessible from both DC and DR.

Deployment Model Definition

1. Fully On-Premises

The complete solution, including the application, management/control plane, processing components, databases and all other components required for full functionality, shall be deployed within the Bank's designated infrastructure at the Primary Data Centre (DC) and Disaster Recovery (DR) Centre.

All such components shall be subject to the HA/DR architecture specified for the respective solution in this RFP. Where N+N Active-Active configuration is specified, the applicable critical components shall be deployed in N+N Active-Active configuration at both DC and DR.

2. SaaS + On-Premise Components

The primary application, management/control plane and associated service shall be provided as a Software-as-a-Service (SaaS) offering hosted by the OEM/CSP. Supporting components required within the Bank's environment for data collection, processing, connectivity, integration, inspection, enforcement or other required functionality may be deployed at the Bank's premises.

All Cloud/SaaS solutions shall have an Aggregator/Collector/Connector Server or VM deployed at both Bank DC and DR, in line with the deployment design and HA requirements of the respective solution, for secure connectivity and integration with the Bank's servers, endpoints and services.

For this deployment model:

The bidder shall provide, license, deploy, configure, integrate, maintain and support all Bank-site/on-premise components required under the proposed OEM architecture, including agents, collectors, brokers, aggregators, sensors, connectors, scanners, enforcers, integrators or equivalent components.

The SaaS service shall comply with the uptime SLA and other service availability requirements specified in this RFP.

Bank-site/on-premise components shall be deployed at both the Primary Data Centre (DC) and Disaster Recovery (DR) Centre in accordance with the HA/DR requirement specified for the respective solution.

Where N+N Active-Active configuration is mandated, all applicable critical Bank-site components shall be deployed in N+N Active-Active configuration at both DC and DR.

The Management Console/control interface shall be accessible from both DC and DR.

3. SaaS + On-Premise Components OR Fully On-Premise

For solutions where both deployment models are expressly permitted, the bidder may propose either:

- SaaS + On-Premise Components, as defined above; or
- Fully On-Premise, as defined above.

The bidder shall clearly identify the deployment model proposed for each solution and provide the complete solution architecture, including the location of all SaaS-hosted and Bank-site components, connectivity dependencies, licensing requirements and DC/DR deployment.

4. Common Requirements

Irrespective of the permitted deployment model, the bidder shall be responsible for providing all components necessary to meet the functional, technical, security, performance, availability and HA/DR requirements specified in this RFP.

Any component required under the proposed OEM architecture for achieving the specified functionality shall be deemed to be part of the bidder's scope, whether or not such component is expressly named in the RFP.
All solutions deployed in Standalone mode shall have independent operational capability at both DC and DR, such that the solution instance at DC can independently manage, monitor and/or process resources hosted at both DC and DR, and vice versa. Applicable data, configurations and solution information shall be synchronized between DC and DR to ensure consistency and continuity of operations.

The bidder shall not exclude any required component from its scope on the grounds that such component is normally supplied as part of the OEM's standard architecture, subscription or SaaS service.
Where HA is mandated for a critical component, partial or selective HA deployment shall not be accepted. The bidder shall ensure that all applicable critical components are deployed in the prescribed HA configuration at both DC and DR.

B. Services

#	Offsite Service	Delivery Model	Frequency	Methodology / How the Service Will Be Performed in the Bank
1	Breach Attack & Simulation (BAS)	Managed Service	Automated; Monthly reporting; Quarterly review	BAS Tool based Services will be integrated with the Bank's approved security environment to continuously simulate controlled attack techniques and validate the effectiveness of security controls. The platform will automatically execute predefined attack simulations without disrupting production systems.
2	Continuous Automated Red Teaming (CART)	Managed Service	Continuous / Automated; Monthly reporting; Quarterly review	The Tool based Services will continuously emulate relevant adversarial techniques against the Bank's approved attack surface and security controls. Scenarios will be configured based on the Bank's threat profile and other requirements as mentioned in the RFP
3	Attack Surface Management (ASM)	Managed Service	Continuous / 24×7; continuous discovery; Monthly/Quarterly reporting	The ASM Tool based Services will continuously discover and monitor the Bank's internet-facing assets. The service will continuously assess exposures

#	Offsite Service	Delivery Model	Frequency	Methodology / How the Service Will Be Performed in the Bank
4	Phishing Simulation	Managed Service	Quarterly / As required	A controlled phishing simulation Tool based Services will be designed based on the Bank's user population, risk profile and security-awareness objectives.
5	Digital Risk Management	Managed Service	Continuous / 24×7; real-time critical alerts; Monthly reporting	The service will continuously monitor relevant phishing sources, fraudulent domains/websites, spoofed pages, malicious email campaigns, and other applicable sources for Bank-related impersonation and phishing activities. The service will continuously monitor public Internet sources, domains, websites, social platforms and other relevant channels for unauthorized use of the Bank's brand
6	Dark Web Monitoring	Managed Service	Continuous / 24×7; real-time critical alerts; Monthly reporting	The service will continuously monitor relevant dark-web sources, underground forums, and other applicable sources for Bank-related information.
7	Threat Intelligence Feed (TIF)	Managed Service	Real-time / Continuous; daily intelligence updates; Monthly reporting	A continuous threat-intelligence feed will provide the Bank with relevant and actionable intelligence. The Bidder shall provide a commercial Threat Intelligence Feed (CTI Feed) as part of the proposed solution. The **feed shall be sourced from one or more commercially licensed Threat Intelligence sources/providers** and shall not be limited to publicly available/open-source intelligence alone.

#	Offsite Service	Delivery Model	Frequency	Methodology / How the Service Will Be Performed in the Bank
8	Threat Hunting Services	Managed Service	At least Monthly; Quarterly comprehensive assessment	Threat Hunting Tool/Platform with managed services for proactive identification of known and unknown threats using IOC, Threat Intelligence, TTP and behavioural-based hunting. Threat hunting will be performed at least monthly using SIEM raw logs, parsed/normalized logs and other relevant security data sources available to the Bank to identify potential undetected threats and suspicious activities.

16.22 Annexure 22A: Bidder's Client References Format

Format for Submission of Client References

To whosoever it may concern

Particulars	Details
Supporting Documents (Mandatory)	As per the Criteria
Additional Documentary Evidence (Any One Mandatory)	As per the Criteria
Client Information	
Client Name	
Client Address	
Name of Contact Person & Designation	
Contact Number of Contact Person	
Email Address of Contact Person	
Project Information	
Name of the Project	
Project Location	
Start Date of Project	
End Date of Project (if completed)	
Current Project Status	☐ Completed ☐ In Progress
Industry / Sector	
Project Size & Commercials	
Value of Single Work Order / Contract (INR Lakhs)	
Number of Branches / Offices Covered	
Scope of Work	
Brief Description of Scope Relevant to PSB Requirement	
Cyber Security Solutions Implemented (Tick Applicable Solutions)	
SIEM	☐ Yes ☐ No
XDR/EDR	☐ Yes ☐ No
SOAR	☐ Yes ☐ No
UEBA	☐ Yes ☐ No
Decoy	☐ Yes ☐ No
Threat Intelligence Platform	☐ Yes ☐ No
Vulnerability Assessment /Vulnerability Management	☐ Yes ☐ No
ITDR	☐ Yes ☐ No
Application Security Testing (SAST/DAST)	☐ Yes ☐ No
Cloud Security Posture Management Tool	☐ Yes ☐ No
CNAPP	☐ Yes ☐ No
CWPP	☐ Yes ☐ No

Particulars	Details
CTEM	☐ Yes ☐ No
Services	
Breach Attack & Simulation	☐ Yes ☐ No
Continuous Automated Red Teaming services	☐ Yes ☐ No
Attack Surface management	☐ Yes ☐ No
Phishing Simulation	☐ Yes ☐ No
Digital risk management	☐ Yes ☐ No
Dark web Monitoring	☐ Yes ☐ No
Threat Intelligence Feed	☐ Yes ☐ No
Threat Hunting services	☐ Yes ☐ No
Evidence Submitted	
Copy of PO / WO / Contract Attached	☐ Yes ☐ No
Client Credential Letter / Email Attached	☐ Yes ☐ No
Client Installation Report / Sign-off Attached	☐ Yes ☐ No
OEM Self-Declaration Attached	☐ Yes ☐ No
Additional Documents Submitted	
Clause-to-Evidence Mapping Matrix	
Document Type (PO/Contract/Credential Letter/Email/OEM Declaration)	
Page Number in the proposal	
Section Number in the proposal	
Sub-Section / Clause No. in the proposal	
Exact Relevant Excerpt from the document type	
Certification by Bidder	We hereby certify that the above information is true and correct and supported by documentary evidence submitted as part of the bid.
Authorized Signatory Name	
Designation	
Signature & Seal	
Date	

Name & Signature of authorised signatory

Seal of Company

16.23 Annexure 22B: OEM Self-Declaration For Credentials

[To be submitted by the OEM on its Letterhead]

RFP Reference No.: _____

RFP Title: _____

To,
General Manager (CISO)
STAFF TRAINING CENTRE PUNJAB AND SIND BANK
Punjab & Sind Bank, CISO cell 3rd Floor,
B-8/232, Naharpur Village Rd, Pocket 8, Sector 3B,
Rohini, Delhi, 110085

We, M/s _____, being the OEM of the proposed solution, hereby certify that the solution mentioned below has been supplied, installed/implemented and maintained/supported, as applicable, at the following client in India:

Particular	Details
Project Name	
Client Name	
Client Category	Scheduled Commercial Bank / PSU / PSE / Government Organization / BFSI/Telecom/Fortune 500 etc.
Solution/Service Category (as per RFP)	Ex. SIEM/SOAR/UEBA/TIP/XDR/ AST/DWM etc.
Solution Name as per OEM	
OEM Name	
Scope Executed	Supply: ☐ Yes ☐ No Installation/Implementation: ☐ Yes ☐ No Maintenance/Support: ☐ Yes ☐ No
Date of Go-Live	
Contract / Project Period	Start: _____ End: _____
Maintenance/Support Status	Current / Completed / Not Applicable

Reference to Client-Issued Evidence, provided by us along with the declaration are:

Document Name	Page No(s.)	Clause/Section	Evidence
Purchase Order / Work Order / Contract			
Client-Issued Supporting Document			

We hereby confirm that the above information is true and correct and that the referenced client-issued document(s) substantiate the stated implementation experience. We further confirm that the solution is/was maintained or supported during the five (5) years preceding the RFP publication date.

For and on behalf of the OEM
OEM Name: _____
Authorized Signatory: _____
Designation: _____
Signature: _____
Date: _____
Place: _____
OEM Seal/Stamp: _____

16.24 Annexure 23: Pre-bid Query format

Pre-Bid Query Format

(Bidders should submit the queries in excel format only)

Ref: RFP No._____ dated _____.

Bidder's Name: _____

S.No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query
1					
2					
3					
4					
5					
-					

16.25 Annexure 24: Proposed Resources CV

Sr No	Parameter	Description	
1	Name & Designation		
2	Proposed Position & Skillset		
4	Educational Qualification		
	Degree Obtained	University/ Institution	Year Obtained
5	Cybersecurity Certification/Qualifications		
6	Professional Experience		
	Designation	Company Name	Year Obtained
7	Total Years of Cyber Security Experience		
8	SOC Solution & services and the relevant Project from the list of solution sought by bank		
10	Experience relevant to the Project Wise		

16.26 Annexure 25: Indicative List of Reports to be Provided to the Bank

The following reports shall be mandatory deliverables. The Bidder may provide additional reports/dashboards based on the threat landscape, risk posture or requirements of the Bank without additional cost.

S. No.	Report / Deliverable	Frequency
1	Daily SOC Situation Report / Daily Security Summary	Daily
2	Critical / Major Security Incident Report	Per incident
3	Weekly SOC Operations Report	Weekly
4	Monthly SOC Performance Report	Monthly
5	Security Incident Trend & Analysis Report	Monthly
6	SLA / KPI / KRA Compliance Report	Monthly
7	Log Source & Monitoring Coverage / Health Report	Monthly
8	SIEM Detection Use Case Effectiveness Report	Monthly; detailed quarterly
9	Alert Quality & False Positive Report	Monthly
10	Threat Intelligence Report	Weekly; consolidated monthly
11	Threat Hunting Report	Per hunt; consolidated monthly
12	MITRE ATT&CK Detection & Coverage Report	Quarterly
13	Detection Gap / Missed Detection Analysis Report	Quarterly and event-driven
14	Security Control Effectiveness Report	Quarterly
15	Vulnerability & Security Exposure Report	Weekly; consolidated monthly
16	Attack Surface / External Exposure Report	Monthly
17	Identity & Privileged Access Security Monitoring Report	Monthly
18	Endpoint / EDR Security Monitoring Report	Monthly
19	Network Security Monitoring Report	Monthly
20	Email Security / Phishing Report	Monthly
21	Data Exfiltration / DLP Monitoring Report	Monthly
22	Cloud Security Monitoring Report	Monthly
23	SOAR / Automation Effectiveness Report	Quarterly
24	Incident RCA & Lessons Learned Report	Per major / critical incident
25	Repeat Incident / Recurrence Analysis Report	Quarterly
26	Compliance & Audit Readiness Report	Quarterly; annual consolidation
27	SOC Capacity, Staffing & Analyst Performance Report	Monthly

28	SOC / SIEM Platform Health & Availability Report	Monthly
29	Executive Cyber Risk Dashboard / Report	Monthly
30	Quarterly Cyber Security Posture Report	Quarterly
31	Annual SOC Effectiveness & Maturity Assessment	Annual
32	Annual Cyber Threat Landscape & Strategic Outlook	Annual

A. Daily SOC Situation Report
   1. Reporting period and overall security posture
   2. Total alerts/events and breakdown by severity
   3. Critical and high-severity alerts/incidents
   4. New, open, closed and aging incidents
   5. SLA breaches and incidents requiring Bank action
   6. Major attack patterns, targeted assets, users and applications
   7. Significant IOCs/IOAs, malware, phishing and data-exfiltration activity
   8. Relevant threat intelligence and emerging threats
   9. Critical vulnerabilities/exposure requiring immediate attention
   10. Actions taken, pending actions, owner and expected closure date

B. Weekly SOC Operations Report
   11. Incident and alert statistics, trends and backlog
   12. SLA performance and exceptions
   13. Top detection rules/use cases and noisy rules
   14. Use-case development, tuning and retirement status
   15. Threat-hunting activities and findings
   16. Threat-intelligence activities and IOCs operationalized
   17. Critical vulnerabilities/exposure and remediation tracking
   18. Open/overdue action items and management escalations

C. Monthly SOC Performance Report
   19. MTTD, MTTR, MTTC and incident closure performance
   20. Critical/high incident triage and escalation SLA performance
   21. SOC/SIEM availability and service disruptions
   22. Alert volume, true-positive/false-positive metrics and alert ageing
   23. Log source coverage and ingestion health
   24. Use-case coverage, effectiveness and tuning
   25. Threat hunting, threat intelligence and SOAR effectiveness
   26. Major incident summary and RCA status
   27. KPI/KRA achievement, month-on-month trend and year-on-year trend
   28. Risks, exceptions, corrective actions and recommendations

D. Log Source & Monitoring Coverage / Health Report including below parameters (but not limited to):-
   - Asset/system, business criticality and expected log source
   - Onboarding/deboarding status
   - Last log received and ingestion status
   - Ingestion volume/EPS where applicable
   - Parser/normalization status
   - Data gaps, outage duration and root cause

- Associated detection use cases
- Monitoring status and remediation ETA

E. SIEM Detection Use Case Effectiveness Report including below parameters (but not limited to):-
- Total active, under-development, under-tuning and retired use cases
- Coverage by asset, security control, business service and MITRE ATT&CK
- Alert volume, true positives and false positives
- Detection effectiveness and incidents generated
- Use cases with no/abnormal triggering
- Tuning completed/pending
- Detection gaps and recommended new use cases

F. Threat Hunting Report including below parameters (but not limited to):-
- Hunt objective and hypothesis
- Threat intelligence/risk basis
- Scope and data sources searched
- MITRE ATT&CK techniques/TTPs
- Findings, affected assets and users
- IOCs/IOAs identified
- Incidents generated or controls triggered
- Detection gaps discovered
- New detections/use cases created from findings
- Recommendations and follow-up actions

G. MITRE ATT&CK Detection & Coverage Report including below parameters (but not limited to):-
- Tactic, technique and sub-technique coverage
- Data sources supporting each detection
- Detection/use-case mapping
- Full/partial/no coverage
- High-risk detection gaps and blind spots
- Techniques requiring additional telemetry or controls
- Recommended remediation and target completion dates

H. Vulnerability & Security Exposure Report including below parameters (but not limited to):-
- New critical/high vulnerabilities and exploited vulnerabilities
- Affected critical assets and internet-facing assets
- Exposure by on-premises and cloud environment
- Vulnerability ageing and remediation status
- SLA breaches and exceptions
- Risk accepted items
- Correlation with active threats/attacks where available

I. Major / Critical Incident Report and RCA including below parameters (but not limited to):-
- Executive summary and incident classification
- Detailed incident timeline

- Attack vector and attack path
- Initial access, persistence, privilege escalation, lateral movement and C2, where applicable
- Affected systems, users, applications and data
- MITRE ATT&CK mapping and IOCs/IOAs
- Containment, eradication and recovery actions
- Root cause and control failures
- Detection/monitoring gaps
- Evidence and forensic findings, where applicable
- Lessons learned, corrective actions and preventive recommendations
- Residual risk and management action plan

J. Executive Cyber Risk / Security Posture Report including below parameters (but not limited to):-
- Overall cyber security posture and risk trend
- Critical/high incidents and material threats
- Top cyber risks requiring management attention
- Critical vulnerabilities and external exposure
- Detection and MITRE coverage gaps
- Security control effectiveness
- SLA/KPI performance
- Open high-risk actions and overdue items
- Key recommendations and next-period priorities

K. Annual SOC Effectiveness & Maturity Assessment including below parameters (but not limited to):-
- Assessment of detection, response, threat hunting, threat intelligence and automation maturity
- SIEM/use-case/process/governance maturity
- Cloud, identity, endpoint, network and data-security monitoring maturity
- MITRE ATT&CK coverage and detection gaps
- Comparison with previous year
- Key risks and capability gaps
- Improvement roadmap with priorities, milestones and measurable outcomes

For and on behalf of [Full Legal Name of Bidder]

Authorized Signatory

Name: _____

Designation: _____

Signature: _____

Date: _____

Place: _____

Company Seal / Stamp

16.27 Annexure 26: Undertaking – Support & Launch Confirmation (on OEM's letterhead)

To,

General Manager (CISO)

Staff Training Centre, Punjab & Sind Bank

CISO Cell, 3rd Floor

B-8/232, Naharpur Village Road, Pocket 8, Sector 3B

Rohini, Delhi – 110085

Date:_____

Dear Sir,

Subject: Undertaking – Support & Launch Confirmation for RFP No. PSB/ HO-CISO CELL/2026-27/RFP_01 dated 09/09/2026 (GeM Bid No. GEM/2026/B/8018719)

We, [OEM Name], being the Original Equipment Manufacturer (OEM) of the products offered under the subject Bid/Tender, hereby confirm and undertake that the proposed Model(s) and Version(s) offered against this Bid:

a) are the latest commercially available and supported Model(s) and Version(s) offered by the OEM for the relevant product category as on the date of submission of the Bid;
b) are not declared End-of-Sale (EoS) as on the date of submission of the Bid; and
c) shall remain supported by the OEM and shall not reach End-of-Life (EoL) / End-of-Support (EoS) during the Contract Period or for a period of six (6) years from the date of product installation, whichever is later.

In the event that any proposed Model(s), Version(s), Software, Firmware or other OEM-supplied product/component reaches or is declared End-of-Sale (EoS), End-of-Life (EoL), End-of-Support (EoS), or otherwise becomes unsupported by the OEM during the applicable support period, the OEM shall, at no additional cost to the Bank, provide and implement an equivalent or upgraded replacement Model/Version/Product/Component that meets or exceeds the technical, functional, security, performance, integration, compatibility, capacity and other requirements of the RFP.

Such replacement shall include, as applicable, all necessary licenses, subscriptions, software/firmware, hardware/components, migration, installation, configuration, integration, testing, data migration and technical support required to maintain continuity of the solution and shall not result in any degradation of the existing functionality or security controls.

Thanking You,

Place: _____

Signature of Authorized Signatory (with OEM seal)

Name of OEM / Signatory:

Designation:

Email ID:

Mobile No:

16.28 Annexure 27: Association with Bank

Declaration regarding Prior Association with the Bank and Pending SLA/Contract

To,
General Manager (CISO)
STAFF TRAINING CENTRE PUNJAB AND SIND BANK
Punjab & Sind Bank, CISO cell 3rd Floor,
B-8/232, Naharpur Village Rd, Pocket 8, Sector 3B,
Rohini, Delhi, 110085
Dear Sir/Madam,

We, [Name of the Bidder], having our registered office at [Address], hereby certify and declare that the following provisions, as stipulated in the RFP, have been duly complied with:

1. Prior/Existing Association with the Bank

We hereby confirm that:

☐ The Bidder / its subsidiary / associate / sister company / holding company has not had any association with the Bank during the past five (5) years and does not have any association with the Bank at present as a service provider on any project.

OR

☐ The Bidder / its subsidiary / associate / sister company / holding company has had / currently has an association with the Bank as a service provider on the following project(s):

Sr. No.	Name of Entity	Relationship with Bidder	Name of Project	Period of Association	Bank Department/Division	Details of Engagement
1						
2						

In case of any such past or existing association, we are submitting along with our bid the satisfactory certificate issued by the Bank, which has been issued/dated after the issuance of the RFP, as required under the RFP.

2. Pending SLA/Contract

We hereby confirm that there is no Service Level Agreement (SLA) or Contract pending to be signed/executed with the Bank for a period of more than six (6) months from the date of issuance of the corresponding Purchase Order (PO).

We hereby declare that the information furnished above is true, complete and correct to the best of our knowledge and belief.

We understand that any misrepresentation or concealment of material facts may result in rejection of our bid and/or such other action as may be deemed appropriate by the Bank in accordance with the terms and conditions of the RFP.

For and on behalf of [Name of the Bidder]
Authorized Signatory: _____
Name: _____
Designation: _____
Company Name: _____
Address: _____
Contact No.: _____
Email ID: _____
Date: _____
Place: _____
Company Seal/Stamp

16.29 Annexure 28 Ownership Declaration and Contractual performance

To
General Manager (CISO)

STAFF TRAINING CENTRE PUNJAB AND SIND BANK

Punjab & Sind Bank, CISO cell 3rd Floor,

B-8/232, Naharpur Village Rd, Pocket 8, Sector 3B,

Rohini, Delhi, 110085

Dear Sir/Madam,

We, M/s [Name of the Bidder], having our registered office at [Complete Address], hereby declare and confirm that none of our:

- Subsidiary company/companies;
- Sister company/companies;
- Associate company/companies;
- Holding company/companies;
- Company/companies having common director(s);
- Company/companies belonging to the same group of promoters/management; or
- Partnership firm(s)/LLP(s) having common partner(s),

is owned by any Director or Employee of Punjab & Sind Bank (PSB).

We further declare that there is no direct or indirect ownership by any Director or Employee of the Bank in any such entity associated with the Bidder, which would result in non-compliance with the eligibility requirements stipulated in the RFP.

We certify that the information provided in this declaration is true, complete, and correct to the best of our knowledge and belief.

We understand that any misrepresentation or concealment of material facts may result in rejection of our bid and/or such other action as may be taken by the Bank in accordance with the terms and conditions of the RFP.

For and on behalf of M/s [Name of the Bidder]
Authorized Signatory: _____
Name: _____
Designation: _____
Company Name: _____
Address: _____
Contact No.: _____
Email ID: _____
Date: _____
Place: _____
Company Seal/Stamp

16.30 Annexure 29: Contract Cancellation / Termination / Rescission / Revocation

SELF-DECLARATION REGARDING CONTRACT CANCELLATION / TERMINATION / RESCISSION / REVOCATION
[To be submitted on the Bidder's Letterhead]

RFP Reference No.: _____
RFP Title: _____
Date of RFP Publication: _____
To
Punjab & Sind Bank
_____

Subject: Self-Declaration regarding Contract / Purchase Order / Award issued by Punjab & Sind Bank
We, M/s _____, having our registered office at _____, hereby declare and confirm that, during the last three (3) years preceding the date of publication of the above-mentioned RFP, no contract, Purchase Order, Letter of intent, work order, or award issued by Punjab & Sind Bank (PSB) to us has been cancelled, terminated, rescinded, or revoked due to non-performance, breach of contractual obligations, or failure to comply with post-award requirements.
We further confirm that:

1. There has been no cancellation, termination, rescission, or revocation of any contract, Purchase Order, work order, letter of intent, or award issued by PSB to us during the aforesaid period on account of our non-performance, breach of obligations, or failure to fulfil post-award requirements.
2. The information furnished in this declaration is true, complete, and correct to the best of our knowledge and belief.
3. We understand that any false, misleading, or incorrect declaration or concealment of any material fact may result in disqualification of our bid, cancellation of the award/contract, forfeiture of applicable securities or payments, and/or such other action as may be permissible under the terms of the RFP and applicable laws.
4. We undertake to promptly notify Punjab & Sind Bank if any information stated in this declaration becomes inaccurate or changes at any stage during the procurement process.

This declaration is submitted in accordance with the eligibility and qualification requirements stipulated in the RFP.

For and on behalf of the Bidder
Name of the Bidder: _____
Authorized Signatory: _____
Name of Authorized Signatory: _____
Designation: _____
Signature: _____
Date: _____
Place: _____
Company Seal / Stamp:

16.31Annexure 30: Compliance with Applicable Labour Laws

SELF-DECLARATION REGARDING Compliance with Applicable Labour Laws

[To be submitted on the Bidder's Letterhead]
RFP Reference No.: _____
RFP Title: _____
Date of RFP Publication: _____

To
Punjab & Sind Bank
_____

Subject: Declaration for Compliance with Applicable Labour Laws
We, M/s _____, having our registered office at _____, hereby declare and undertake that, if awarded the contract pursuant to the above-mentioned RFP, we shall comply with all applicable labour and employment laws, rules, regulations, notifications, and statutory requirements as applicable from time to time in respect of the personnel deployed for execution of the services under the contract.
This declaration is submitted in accordance with the eligibility and qualification requirements stipulated in the RFP.

For and on behalf of the Bidder
Name of the Bidder: _____
Authorized Signatory: _____
Name of Authorized Signatory: _____
Designation: _____
Signature: _____
Date: _____
Place: _____
Company Seal / Stamp:

16.32 Annexure 31- Conflict of Interest and IT Security Vendor Restriction

DECLARATION REGARDING CONFLICT OF INTEREST AND IT SECURITY VENDOR RESTRICTION

[To be submitted on the Bidder's Letterhead]

RFP Reference No.: _____
RFP Title: _____
Date of RFP Publication: _____

To
Punjab & Sind Bank
[Address of the Bank / RFP Issuing Authority]

Subject: Declaration regarding Conflict of Interest and IT Security Vendor Engagement

We, M/s _____, having our registered office at _____, hereby declare and confirm that, in connection with our participation in the above-mentioned RFP, we shall maintain the required independence and shall not have any conflict of interest that may adversely affect the confidentiality, integrity, objectivity, or security of the services to be provided to Punjab & Sind Bank (PSB).

We hereby confirm and undertake that:

1. The successful bidder, its subsidiary, associate, sister concern/company, holding company, or any entity under common control or management shall not be the IT Security vendor of Punjab & Sind Bank under any existing contract during the tenure of the contract awarded pursuant to this RFP.
2. We acknowledge that a bidder may participate in both the NextGen SOC RFP and the IT Security Solution & Services RFP bearing GeM Bid Nos. GEM/2026/B/7936763 and GEM/2026/B/7752177, respectively.
3. A Bidder participating in the NEXTGEN SOC RFP and either or both of the ongoing IT Security RFPs (GEM/2026/B/7936763 and GEM/2026/B/7752177) shall be eligible for consideration under NEXTGEN SOC or the IT Security RFP(s), as applicable, but not both. If a Bidder participates in NEXTGEN SOC RFP and any IT Security RFP, the RFP whose commercial bid is opened first shall take precedence, and the Bidder shall not be considered for evaluation or award under the other RFP, the NEXTGEN SOC RFP and either or both IT Security RFPs). Participation in both IT Security RFPs (GEM/2026/B/7936763 and GEM/2026/B/7752177) shall not, by itself, attract this restriction.
4. The RFP between NextGEN SOC RFP and the IT Security RFP(s) under which the Bidder's commercial bid is opened first shall be considered for further evaluation and award. Thereafter, the Bidder shall become ineligible for further evaluation or award under the other RFP(s). Accordingly, the commercial bid under the other RFP(s), if not yet opened,

shall not be opened; and if already opened, shall not be considered for further evaluation or award. The decision of Punjab & Sind Bank in this regard shall be final and binding.

5. We shall ensure that there is no direct or indirect conflict of interest between the services being provided under this RFP and any IT Security-related services being provided to PSB by the Bidder or by any of its subsidiary, associate, sister concern/company, holding company, or other entity under common control or management.
6. We shall promptly disclose to PSB any actual, potential, or perceived conflict of interest that arises at any stage during the procurement process or during the tenure of the contract.
7. In the event that the Bidder or any of the entities referred to above becomes an IT Security vendor of PSB during the contractual period, we shall immediately inform PSB and comply with the Bank's directions regarding resolution of such conflict, including cessation of the conflicting engagement, wherever required by the Bank.
8. We understand and acknowledge that PSB shall have the right to determine whether any actual, potential, or perceived conflict of interest exists and whether such conflict is capable of being satisfactorily resolved.
9. We further acknowledge that any false, incomplete, or misleading declaration, non-disclosure of a material conflict of interest, or breach of this undertaking may result in rejection/disqualification of our bid, cancellation of the award, termination of the contract, and/or such other action as may be available to PSB under the RFP, contract, and applicable laws.
10. We undertake to provide, upon request by PSB, such information, declarations, or supporting documents as may be reasonably required by the Bank to verify compliance with this undertaking.

We hereby certify that the information provided above is true, complete, and correct to the best of our knowledge and belief, and we undertake to comply with the above conditions throughout the procurement and contractual period.

For and on behalf of the Bidder
Name of the Bidder: _____
Authorized Signatory: _____
Name of Authorized Signatory: _____
Designation: _____
Signature: _____
Date: _____
Place: _____
Company Seal / Stamp:

16.33 Annexure 32 – OEM Functional Compliance Declaration

RFP No.: _____
Name of Bidder: _____
Name of OEM: _____

We hereby confirm and declare that:

1. The proposed products, solutions and services have been evaluated against the requirements specified in Appendix 1A & 1C– Functional Compliance Sheet.
2. The compliance status provided in Appendix 1A as S – Standard, C – Customization is true and accurate.
3. The duly filled and signed Functional Compliance Sheet submitted in both Excel and PDF formats forms
4. All functionalities marked as compliant shall be available within the proposed product/version and scope.
5. The proposed solution shall achieve a minimum 85% functional compliance scoring for each individual product/solution/service, as specified in the RFP.
6. All required licenses, modules, integrations and dependencies necessary to deliver the committed functionality have been identified in the proposal.
7. Supporting documents such as OEM datasheets, product manuals, technical documentation and product feature references have been provided.
8. The Bank may verify the claimed functionality through demonstration, PoC, technical validation or UAT.
9. We undertake to deliver all commitments made in Appendix 1A & 1C within the timelines specified by the Bank without impacting on the Bank's project/UAT schedule.

For OEM
Name: _____
Designation: _____
Signature: _____
Date: _____
Seal: _____

16.34 Annexure 33: Back-to-back support/backlining confirmation

To,
General Manager (CISO)

STAFF TRAINING CENTRE PUNJAB AND SIND BANK

Punjab & Sind Bank, CISO cell 3rd Floor,

B-8/232, Naharpur Village Rd, Pocket 8, Sector 3B,

Rohini, Delhi, 110085

Dear Sir/Madam,

We, [Name of the Bidder], having our registered office at [Address], hereby certify and declare the following:
We confirm that we have a valid back-to-back support arrangement with the proposed OEM(s) for the solutions/services offered under this RFP and shall ensure OEM support throughout the contract period for meeting the terms of the RFP. A formal back-to-back support agreement with the respective OEM(s) shall be executed/signed, to ensure continued OEM support throughout the contract period inline with the requirement stated in the RFP.
We undertake to provide valid documentary evidence of the OEM support arrangement/authorization upon request by the bank.

For and on behalf of [Name of the Bidder]
Authorized Signatory: _____
Name: _____
Designation: _____
Company Name: _____
Address: _____
Contact No.: _____
Email ID: _____
Date: _____
Place: _____
Company Seal/Stamp

16.35 Annexure 34: Insurance Surety Bond against EMD

(To be executed on Non-Judicial Stamp Paper of Appropriate value)

Insurance Surety Bond No..... Date:.....

(Name of the RFP:)

To: (Name and address of The Beneficiary/ Bank)

WHEREAS (Name of Bidder) (hereinafter called "the Bidder") has submitted its Bid dated (date of bid) for the Earnest Money Deposit for the captioned RFP _____ (hereinafter called "the Bid") KNOW ALL PERSONS by these present that We (name of Insurance Company) (address of Insurance Company) (hereinafter called "the Surety"), are bound unto Punjab & Sind Bank, _____, constituted under the provisions of Banking Companies (Acquisition & Transfer of Undertakings) Act, 1970, having its Head Office at Punjab & Sind Bank, IT Department, Plot No. 151, Sector 44, Gurugram, 122003, hereinafter called "the Beneficiary/ Bank") for the sum of..... (amount), for which payment well and truly to be made to the said Beneficiary/ Bank, the Surety binds itself, its successors and assigns by these presents.

THE CONDITIONS of this obligation are as follows:

1. If the Bidder (a) withdraws or modifies its Bid during the period of bid validity, or (b) adopts corrupt or collusive or coercive or fraudulent practices or defaults under Integrity Pact.
2. If the Bidder, having been notified of the acceptance of its Bid by the Beneficiary/ Bank during the period of bid validity.
    a. fails or refuses to sign the Contract Agreement when required, or
    b. fails or refuses to submit the performance security in accordance with the Tender Documents.

We undertake to pay to the Beneficiary/ Bank up to the above amount upon receipt of its first written demand, without the Beneficiary/ Bank having to substantiate its demand, provided that in its demand the Beneficiary/

Bank will mention that the amount claimed by it is due, owing to the occurrence of one or both of the two above-named CONDITIONS, and specifying the occurred condition or conditions.

The Surety declares that this Insurance Surety Bond is issued by the..... (name of Insurance Company) as per the applicable rules and regulations of Insurance Regulatory Development Authority of India (IRDAI).

This Insurance Surety Bond will remain in force up to and including (date 90 days after the period of bid validity), and any demand in respect thereof must reach the Surety not later than the above date.

INSTRUCTIONS FOR EXECUTION OF INSURANCE SURETY BOND FOR EARNEST MONEY DEPOSIT

1. Insurance Surety Bond for Earnest Money Deposit should be executed on non-judicial Stamp papers of requisite value in accordance with the stamp Act if applicable to that particular state of Indian Union country of executing Insurance Company, where executed. In case the

same is issued by an International Insurance Company (it should be registered under insurance Act 1938 or as amended from time to time and approved by the Insurance Regulatory Development Authority of India (IRDAI)) the law prevalent in the country of execution shall prevail for the purpose of Stamp Duty on the Insurance Surety Bond. However, in such a case, the Insurance Surety Bond for Earnest Money Deposit shall be got confirmed by the Bidder through any Indian Scheduled/Nationalized Insurance Company.

2. The executing officers of the Insurance Surety Bond for Earnest Money/Bid Security shall clearly indicate in (block letters) his name, designation, Power of Attorney No./Signing Power No. as well as telephone/ fax numbers with full correspondence address of the issuing Guarantee etc.

3. Each page of the Insurance Surety Bond for Earnest Money Deposit shall be duly signed/initialled by the executing officers and the last page shall be signed in full, indicating the particulars as aforesaid (sub-para 2) under the seal of the Insurance Company.

4. Stamp paper shall be purchased in the name of Insurance Company counting the Insurance Surety Bond, after the date 'Notice Inviting Tender', not more than six months prior to execution/issuance of the Insurance Surety Bond. The name of the purchaser should appear at the back side of stamp paper in the Vendors Sign. The issuing insurance Company shall be requested independently for verification/confirmation of the Insurance Surety Bond issued, non-confirmation of which may lead to rejection of 'Insurance Surety Bond'

5. Irrevocable, valid and fully enforceable Insurance Surety Bond in favour of the Beneficiary/ Bank (Name of Beneficiary/ Bank) issued by any Insurance Company registered under Insurance Act amended from time to time and approved by the Insurance Regulatory Development Authority of India (IRDAI) in Indian currency (INR) only is acceptable to the Beneficiary/ Bank.

6. Insurance Surety and for Bid security in original shall be submitted along with the Bid. However, the Issuing Insurance Company shall submit an unstamped duplicate copy of Insurance Surety Bond directly by registered post (A.D.) to the Beneficiary/ Bank (authority inviting tenders) with forwarding letter.

or and on behalf of the Insurance Company

in the capacity of

_____

Common Seal of the Insurance Company with complete address including Tel. Nos./e-Mail Id. Staff Authority No. of the officer of the Insurance Company/Signatory.

16.36 Annexure 35: OEM Compliance & Action Taken Report (ATR)

OEM Name and Address:

_____

_____

Submitting for (Bank Name and Address):_____

_____

_____

_____

_____

Note: Draft Format for submissions by OEMs/Technology Providers to Banks pursuant to CERT-In Guidelines regarding AI-Accelerated Vulnerability Protection and Response Requirements dated 10.06.2026. Bank can do the necessary modifications in the format as per their requirements and compliance policies.

A. Executive Summary

Item	Status
a. Overall Compliance Status	Compliant / Partially Compliant / Non-Compliant
b. Number of Critical Vulnerabilities	
c. Number of High Vulnerabilities	
d. Zero-Day Notifications Pending	
e. Pending Patches	
f. Security Incidents (Last 12 Months)	
g. SDL Compliance	
h. Last Independent Assessment	
i. AI Testing Performed	

1. Security Compliance Commitment

Compliance Area	Compliance Status	Remarks
A. Security Compliance Requirements		
a. Continuous Vulnerability Assessment		
b. Immediate Disclosure of Critical and High-Severity Vulnerabilities		
c. Zero-Day Vulnerability Protocol		
d. AI-Assisted Security Testing Certification		
B. Accelerated Patch Management and Deployment		
a. Patch Development and Compensatory Controls with Indicative Timelines		
b. Patch Deployment Support		
c. Automated Patch Notification		
C. Secure Development Lifecycle (SDL) Compliance		
D. Credential and Access Management		
F. Incident Response and Transparency		
G. Actionable Deliverables Required from OEMs and technology providers		
H. Secure-by-Design compliance		
I. SBOM availability and periodic updates		
J. AI Model Security Assessment (where applicable)		
K. Software Supply Chain Security		
L. Third-party/ Open-Source Component Governance		
M. Compliance with RBI/CERT-In advisories		
N. Secure Configuration Baselines		

2. Product Security Posture Assessment Report

**The assessment should also include AI-assisted testing readiness, SDL compliance status, and credential hygiene verification.*

Product & Version	Known Vulnerabilities	CVSS Severity Scores	Patch Status	Exposed attack surfaces, AI related Risks and exploitation exposure	Mitigation Measures	CVE Reference	Active Exploitation Observed (Yes / No)	Known Exploited Vulnerability	Internet Facing (Yes/ No)	Business Criticality	Remarks

3. Software Bill of Materials (SBOM)

Component	Version	Supplier	Purpose	Known Vulnerabilities	End-of-Support Date	End-of-Life Date	License Type	Criticality	Supplier Risk Rating

4: Hardware/Cryptographic/AI /Quantum Components Inventory

Component Type	Component Name	Version	Purpose	Security Impact	PQC Ready (Yes/ No)	FIPS (Federal Information Processing Standards) 140-2 / FIPS 140-3 Validation Status (Yes/No/N.A.)	Crypto Algorithm Used	AI Model Name	AI Model Version

5: Vulnerability Remediation Action Plan

CVE ID	CVE Publication Date	CVSS Severity Ratings	Affected Version	Exploitation Status	Patch Availability	Interim Mitigation Measures	Testing Requirements	Deployment Timelines

Rollback Procedures	Operational Impact Considerations	Bank Risk Rating	Temporary Workaround	Compensating Controls	Target Closure Date	Actual Closure Date

6: Zero-Day Vulnerability Notification Report

Date Identified	Affected Product	Indicators of Compromise (IOC) Shared	Mitigation Issued	Patch ETA	Detection Source

Vendor Advisory Reference	CERT-In Reference	Threat Intelligence Reference	Severity	Status

7: Patch Advisory & Remediation Status

Vulnerability Details	Severity	Patch Release Date	Deployment Guidance Shared	Patch Testing Completed	Rollback Guidance Shared	Rollback Tested	Downtime Required	Customer Action Required	Status

8: Continuous Security Assessment & Assurance Report

Assessment Type	Assessment Date	Assessment Agency	Assessment Scope	AI-Assisted Assessment (Yes / No)	Penetration Testing Date	Key Findings	Risk Rating	Remediation Status

9: SDL Compliance Certification

SDL Practices	Certification Details	DevSecOps Implemented	Code Review Automation	Comments

10: Security Incident Notification Report

Incident Reference	Root Cause	Impact	Containment Action	Recovery Status	CERT-In Reporting Status	RCA Completion Date	Lessons Learnt	Corrective Actions	Preventive Actions

11: Cybersecurity Liaison & Escalation Matrix

Role	Name	Designation	Email	Contact Number	Availability

12: AI Security Readiness Declaration

The OEM shall submit a declaration confirming the implementation of appropriate AI security governance and assurance measures for AI-enabled products, services and software development practices, wherever applicable. The declaration shall, at a minimum, include the following aspects:

- AI-assisted Secure Software Development Lifecycle (Secure SDLC);
- AI Model Risk Assessment;
- AI Threat Modelling;
- Prompt Injection Testing;
- AI Red Teaming;
- AI Security Monitoring;
- AI Supply Chain Review;
- Model Poisoning Assessment; and
- AI Governance Framework.

13. Source Code Assurance Declaration

The OEM shall submit a declaration confirming that appropriate secure software development and source code assurance practices have been implemented for the products and services supplied to the Bank, wherever applicable. The declaration shall, at a minimum, include the following aspects:

- Secure Code Review;
- Static Application Security Testing (SAST);
- Dynamic Application Security Testing (DAST);
- Software Composition Analysis (SCA) / Dependency Analysis;
- Independent Security Review of the source code and application security controls; and
- Verification and remediation of identified source code vulnerabilities prior to product release.

Mandatory Attachments

- Independent Security Assessment Summary Reports
- VAPT/BAS Summary Reports
- SDL Compliance Certificates
- Latest SOC 2 Report
- ISO 27001 Certificate
- Secure Development Policy
- Pen Test Executive Summary
- AI Security Assessment Report (if AI enabled)
- Product Security Whitepaper
- Additional documents if any

Management Attestation

The undersigned certifies that the information furnished in this report is accurate, complete and reflects the current security posture of the products/services supplied to the Bank. The OEM confirms compliance with applicable CERT-In requirements, vulnerability disclosure obligations, incident reporting obligations, patch management requirements and security assurance commitments.

Authorized Signatory

Name:
Designation:
Date:
(Organization Seal)

	A	B	C	D	E
1	**S. No**	**Solution Name**	**Maximum Mark Allocated**	**Maximum Mark Obtained**	**Respective Solution Compliance (%)**
2	1	**SIEM**	**1530**		
3	2	**SOAR**	**680**		
4	3	**UEBA**	**280**		
5	4	**XDR**	**1160**		
6	5				
7	6	**Application Security Testing**	**920**		
8	7	**Decoy**	**290**		
9	8	**VA - VM**	**890**		
10	9	**ITDR**	**380**		
11	9	**CSPM**	**250**		
12	10	**Threat Intelligence Platform**	**550**		
13	11	**CNAPP**	**560**		
14	12	**CWPP**	**500**		
15	14	**CTEM**	**550**		
16		**GRAND TOTAL**	**6930**	**0**	
17	**Instructions**				
18	**Maximum Marks**	**Compliance (S/C)**	**Maximum Mark**		
19	10	**S (Standard):**	This indicates that the requirement is covered by the standard product functionality. It includes features available out-of-the-box, as well as those achievable through parametrization or rules configuration.		
20	3	**C (Customization):**	Requirements marked as C (Customization) go beyond what is available or possible through standard product configuration. Customization involves: Development of custom code Creation of new functionalities or interfaces Modifications that may impact upgrade paths or require specific deployment and testing cycles User interface enhancements or custom-built screens Creation of entirely new functionality not supported by the base product		
21					
22	**S.No**	**Instruction**			
23	1	Bidder must mandatorily mention the exact page number & clause or section reference from their submitted technical proposal or OEM product documentation which demonstrate compliance with each criteria (specification). Any Response marked as compliance without a valid page reference/section reference, shall be treated as in-complete and may be liable for rejection/scoring penalties			

	A	B	C	D	E
1	**S. No**	**Solution Name**	**Maximum Mark Allocated**	**Maximum Mark Obtained**	**Respective Solution Compliance (%)**
24	2	Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or " Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product			
25	3	All Regulatory guidelines requirements as on the date of Bid Submission should be complied from day 1. Bidder/OEM is also required to comply with all the guidelines (regulatory & statutory) issued during the contract period			
26	4	In case bidder has provided the response which is neither "S" or "C". The requirement shall be considered as "No"or "N", the bid shall be liable for rejection			
27	5	All the above mentioned features should be available form the day 1.			

All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution

S.No.	Requirement Area	CSP/SaaS Compliance Requirement	Vendor Compliance (Y/N)	Reference Page Number/Clause Number in Bidder's Technical documents	Vendor's Remarks
1	SaaS Deployment	OEM Confirms that the proposed solution is deployed on a Cloud/SaaS architecture and supports on-demand scaling and seamless failover of instances.			
2	CSP Eligibility	OEM Confirms that the proposed CSP is a valid MeitY-empanelled Cloud Service Provider.			
3	Data Centre Locations	OEM Confirms that the CSP provides two data centre locations for the proposed service.			
4	India Hosting	OEM Confirms that all Bank data, cloud servers and applicable processing infrastructure are hosted within India.			
5	Data Processing Location	OEM Confirms that all data functions and processing relating to the Bank are performed within the boundaries of India.			
6	Data Transfer Outside India	OEM Confirms that Bank data will not be transferred, replicated or processed outside India by any mechanism.			
7	Primary & Secondary DC	OEM Confirms the physical location of Primary and Secondary Cloud Data Centres in India.			
8	DR Location	OEM Confirms that OEM will Deliver 99.99 % uptime throughout the contract period			
9	India Region Gateway	OEM Confirms availability of local India-region gateways from Day 1.			
10	Geographic Expansion	OEM Confirms that the solution can subsequently support additional geographies/countries where required without compromising the India hosting requirement for Bank data.			
11	Single Tenancy	OEM Confirms they will dedicated tenant to bank.			
12	Logical Separation	OEM Confirms strict, logical separation such that no other tenant can access, modify or otherwise interact with Bank data.			
13	BYOK	OEM Confirms that the proposed solution would fully secure through Bank-controlled BYOK encryption and exclusive PSB admin authority.			
14	Tenant-Specific IAM	OEM Confirms they will put in place Access & Governance i.e., Strict Role-Based Access Control (RBAC), and Zero Trust, time-bound access to prevent unauthorized access/viewing			
15	Zero Trust	OEM Confirms data is secured using TLS 1.2+ in transit and AES-256 encryption at rest			
16	Cloud Landing Zone	OEM Confirms deployment through CSP-native guardrails / secure cloud Landing Zone for compliance, logging and resource segregation.			
17	Data Protection	OEM Confirms that all Bank data stored in the cloud is protected through appropriate privacy and security controls.			
18	Data Privacy Laws	OEM Confirms compliance with applicable Government of India, RBI and other regulatory requirements relating to data privacy and protection.			
19	Regulatory Changes	OEM Confirms that necessary enhancements required due to changes mandated by regulators/Government of India will be implemented without additional cost to the Bank, where required by the RFP.			
20	Data Confidentiality	OEM Confirms responsibility for confidentiality and privacy of Bank data and application data.			
21	Data Custodianship	OEM Confirms that the CSP acts only as custodian of Bank data with no independent rights to access, inspect, process, or utilize Bank data			
22	Data Ownership	OEM Confirms that ownership of all Bank data remains with the Bank.			
23	Data Usage Restriction	OEM Confirms that Bank data will not be used for marketing, data mining or any other CSP/OEM purpose without bank's written permission			
24	PII Protection	OEM Confirms that sensitive information/PII is anonymised, masked, tokenised or encrypted in the cloud.			
25	PII Data Sharing	OEM Confirms that Bank PII will not be shared with unauthorised parties or external entities.			
26	Encryption at Rest	OEM Confirms encryption of Bank data at rest.			
27	Encryption in Transit	OEM Confirms encryption of Bank data in transit.			
28	Encryption in Processing	OEM Confirms capability to protect/encrypt data during processing/use where applicable.			
29	Field-Level Encryption	OEM Confirms availability of field-level encryption for sensitive information.			
30	End-to-End Encryption	OEM Confirms support for end-to-end encryption; All Bank telemetry and logs are encrypted in transit from source agents and collectors using TLS 1.2/1.3 and encrypted at rest			

S.No.	Requirement Area	CSP/SaaS Compliance Requirement	Vendor Compliance (Y/N)	Reference Page Number/Clause Number in Bidder's Technical documents	Vendor's Remarks
31	TLS	OEM Confirms use of TLS 1.2 or higher for information exchanged with Bank interfaces/external parties.			
32	Access Control	OEM Confirms system and software access control and administration mechanisms.			
33	Default Deny	OEM Confirms implementation of a Default Deny All access philosophy wherever applicable.			
34	Privileged Access	Provide details of privileged access controls for CSP administrators and support personnel for bank's tenant as and when required by bank.			
35	MFA	OEM Confirms MFA for privileged/administrative access.			
36	Bank Authentication	OEM Confirms ability to integrate with the Bank's authentication framework / Active Directory where applicable.			
37	SSO	OEM Confirms support for Single Sign-On / built-in SSO capabilities.			
38	Password Policy	OEM Confirms compliance with the Bank's applicable password management policy.			
39	ISO 27001	OEM Confirms that the proposed cloud/service environment conforms to ISO 27001 along with annual SOC 2 Type II audit reports			
40	ISO 27017	OEM Confirms conformity/certification against ISO 27017 for cloud security controls.			
41	ISO 27018	OEM Confirms conformity/certification against ISO 27018 for protection of PII in cloud environments.			
42	SOC 2	OEM Confirms SOC 2 certification/report availability.			
43	SSAE/SOC	OEM Confirms availability of applicable SSAE/SOC assurance reports.			
44	SOC 2 Type II	OEM Confirms that the cloud security solution is SOC 2 Type II certified.			
45	Compliance Certifications	OEM Confirms that all applicable compliance certifications can be provided to the Bank whenever requested.			
46	CERT-In Auditor	OEM Confirms that applicable VAPT/API assessment/source-code audit is certified/conducted by a CERT-In empanelled auditor. Such reports/evidence shall be made available to the Bank upon the Bank's request			
47	API Security Assessment	OEM Confirms regular API security assessment.			
48	Source Code Audit	OEM Confirms source-code security assessment where applicable.			
49	CERT-In Advisories	OEM Confirms monitoring of CERT-In advisories and remediation of applicable vulnerabilities.			
50	Data Retention	OEM Confirms compliance with Bank-defined data retention requirements.			
51	Data Archiving	OEM Confirms support for Bank-defined archiving requirements.			
52	Data Masking	OEM Confirms support for data masking/encryption as per Bank requirements.			
53	Data Destruction	OEM Confirms secure destruction/purging of Bank data upon Bank instruction.			
54	Slack Data	OEM Confirms that destruction includes data residing in slack space/data structures and media, where applicable.			
55	Deletion/ Destruction	OEM Confirms that the applicable Bank data has been securely and permanently destroyed/deleted in accordance with the agreed data retention and destruction requirements.			
56	Multi-Site Resilience	OEM Confirms capability for multi-site deployment/fault tolerance for business continuity.			
57	High Availability	OEM Confirms high availability of the cloud service and infrastructure.			
58	Failover	OEM Confirms seamless failover between cloud instances/components.			
59	DC/DR Security	OEM Confirms secure cloud infrastructure across DC and DR/secondary site as applicable.			
60	Business Continuity	Provide BCP/DRP arrangements covering the CSP/SaaS service.			
61	DR Testing	OEM Confirms periodic DR/BCP testing and provide latest test evidence.			
62	Continuous Monitoring	OEM Confirms continuous monitoring of the cloud environment and security events.			
63	Audit Logging	OEM Confirms comprehensive logging of security, administrative and relevant system activity.			
64	Access Monitoring	OEM Confirms monitoring of user/administrator access.			
65	Threat Monitoring	OEM Confirms threat/security monitoring capability.			
66	Log Protection	OEM Confirms protection against unauthorised modification/deletion of logs.			
67	Incident Response	OEM Confirms defined incident response and reporting procedures.			
68	Forensic Support	OEM Confirms provision of forensic investigation support to the Bank when required.			

S.No.	Requirement Area	CSP/SaaS Compliance Requirement	Vendor Compliance (Y/N)	Reference Page Number/Clause Number in Bidder's Technical documents	Vendor's Remarks
69	Application Access	OEM Confirms protection of application executable files/source code against unauthorised access/theft.			
70	Tenant Privacy	For native multi-tenancy, OEM Confirms privacy of data across tenants through appropriate access controls.			
71	API Security	OEM Confirms APIs can be invoked only by authorised applications/entities.			
72	Transaction Logging	OEM Confirms extensive audit logging of transactions and important non-transactional activities.			
73	Data Purging	OEM Confirms mechanism to purge old data after archival while maintaining transactional integrity.			
74	Government Data Requests	OEM Confirms process for handling government requests for Bank/customer data.			
75	Invalid Requests	OEM Confirms that invalid government demands will be resisted/challenged or shall be communicated to the bank in advance			
76	Indian Law	OEM Confirms that the bidder/CSP complies with applicable laws of India.			
77	RBI Compliance	OEM Confirms compliance with applicable RBI requirements/guidelines.			
78	CERT-In Compliance	OEM Confirms compliance with applicable CERT-In directives/security requirements.			
79	MeitY Compliance	OEM Confirms compliance with applicable MeitY requirements and empanelment requirement.			
80	PII Standards	OEM Confirms compliance with ISO 27018 and applicable Indian PII/data protection requirements.			
81	Regulatory Updates	OEM Confirms ongoing compliance when applicable regulatory/security requirements are amended.			
82	Right to Audit	OEM Confirms that the Bank has the right to audit the CSP/SP's compliance with the agreement.			
83	Audit of Premises	OEM Confirms Bank/auditor/regulator access to relevant CSP premises and records where Bank data is held, subject to applicable legal/security conditions.			
84	Regulator Audit	OEM Confirms audit rights for Bank-appointed auditors and regulators.			
85	Data Destruction Audit	OEM Confirms Bank's right to audit data destruction/purging practices.			
86	Cloud Service Availability	OEM Confirms the cloud/web security service provides 99.99% monthly uptime SLA.			
87	India Data Centres from Day 1	OEM Confirms cloud service is hosted in different locations with data centres based in the India region from Day 1.			
88	SOC 2 Type II	OEM Confirms cloud security solution is SOC 2 Type II certified.			
89	Regulatory Data Deportation	OEM Confirms support for exporting/deporting Bank data from cloud when required due to regulatory/statutory mandates, without additional cost to Bank.			

CNAPP						
S.No.	**Functional Specification**	**Updated in Addendum**	**Maximum Marks**	**Compliance (S/C)**	**Calculated Score**	**Remarks**
The OEM shall submit mandatory compliance with the Cloud Deployment requirements along with the Functional Specifications of the proposed solution.						
1	The proposed Cloud-Native Application Protection Platform (CNAPP) shall provide an integrated capability to identify, assess, correlate, prioritize and manage security risks associated with cloud-native applications and their application components throughout the application lifecycle.	RFP Requirement is applicable	10	Select	0	
2	The solution shall provide centralized visibility of cloud-native applications, application components, dependencies, services, APIs, containers, Kubernetes resources, serverless functions and associated application relationships, as supported by the respective cloud platform.	RFP Requirement is applicable	10	Select	0	
3	The solution shall support security assessment across the Bank's multi-cloud and hybrid-cloud application environment, including major public-cloud platforms such as AWS, Microsoft Azure and Google Cloud Platform etc.	RFP Requirement is applicable	10	Select	0	
4	The solution shall provide application-centric risk analysis by correlating relevant application components, dependencies, vulnerabilities, identities, permissions, configurations, exposure and relationships to identify potential security risks.	RFP Requirement is applicable	10	Select	0	
5	The solution shall provide capabilities to assess identity and entitlement risks associated with cloud-native applications, including excessive, unused, inappropriate or risky permissions.	RFP Requirement is applicable	10	Select	0	
6	The solution shall provide visibility into relevant human and machine identities, service accounts, roles, application identities and permissions associated with cloud-native applications.	RFP Requirement is applicable	10	Select	0	
7	The solution shall identify excessive privileges, inappropriate access, unused permissions and risky combinations of permissions that may increase the risk of unauthorized access to cloud-native applications or associated resources.	RFP Requirement is applicable	10	Select	0	
8	The solution shall provide attack-path analysis or equivalent contextual risk analysis to identify potential paths from external exposure, compromised identities, vulnerable components or other attack vectors to critical applications, services or data.	RFP Requirement is applicable	10	Select	0	
9	The solution shall correlate relevant application vulnerabilities, identity risks, exposure, configuration context, dependencies and application relationships to determine overall application-security risk.	RFP Requirement is applicable	10	Select	0	
10	The solution shall provide risk-based prioritization using factors such as severity, exploitability, exposure, business criticality, identity privileges, application context and potential impact.	RFP Requirement is applicable	10	Select	0	
11	The solution shall provide capabilities to map applications to their underlying cloud services, resources, identities, dependencies and application components, enabling application-level security analysis.	RFP Requirement is applicable	10	Select	0	
12	The solution shall support business-context enrichment of applications and application components, including ownership, business criticality, environment and other organizational attributes.	RFP Requirement is applicable	10	Select	0	
13	The solution shall provide security assessment of application deployment definitions, Infrastructure-as-Code (IaC), infrastructure templates and/or equivalent configuration artifacts used during the application lifecycle.	RFP Requirement is applicable	10	Select	0	
14	The solution shall identify security and compliance risks in applicable application deployment configurations before production deployment or implementation, wherever technically feasible.	RFP Requirement is applicable	10	Select	0	
15	The solution shall support integration with application development and deployment workflows, including CI/CD pipelines and/or equivalent mechanisms, to identify, communicate and track application-security risks during the development lifecycle.	RFP Requirement is applicable	10	Select	0	

CNAPP						
S.No.	Functional Specification	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
16	The solution shall support integration with relevant source-code repositories, development tools, build systems, CI/CD platforms and security workflows, either natively or through supported connectors/APIs.	RFP Requirement is applicable	10	Select	0	
17	The solution shall identify security risks and known vulnerabilities associated with third-party, open-source and externally sourced software components and dependencies used by cloud-native applications.	RFP Requirement is applicable	10	Select	0	
18	The solution shall provide visibility into application dependencies and software components and shall identify affected applications where a vulnerable component or dependency is detected.	RFP Requirement is applicable	10	Select	0	
19	The solution shall provide security assessment of containerized application components during development, build, deployment or pre-runtime stages, including identification of known vulnerabilities and insecure configurations, as applicable.	RFP Requirement is applicable	10	Select	0	
20	The solution shall provide security assessment capabilities for Kubernetes and/or equivalent cloud-native orchestration environments, including application deployments, permissions, services, interfaces and relevant configurations.	RFP Requirement is applicable	10	Select	0	
21	The solution shall provide security assessment capabilities for serverless applications and functions, including dependencies, permissions, triggers, interfaces and relevant application configurations, where supported by the cloud platform.	RFP Requirement is applicable	10	Select	0	
22	The solution shall provide security visibility for cloud-native APIs and application interfaces, including risks related to exposure, authentication, authorization, access control and relevant configurations, where supported.	RFP Requirement is applicable	10	Select	0	
23	The solution shall identify security risks associated with application-to-application and application-to-service communication, including inappropriate trust relationships and excessive access.	RFP Requirement is applicable	10	Select	0	
24	The solution shall provide visibility into application access to sensitive or critical data and identify security risks arising from inappropriate application access, exposure or relationships, where supported.	RFP Requirement is applicable	10	Select	0	
25	The solution shall identify vulnerable application components that are reachable, exposed or potentially exploitable within the application's dependency or relationship graph, where such analysis is supported.	RFP Requirement is applicable	10	Select	0	
26	The solution shall provide application-centric vulnerability prioritization, enabling security teams to distinguish vulnerabilities that present meaningful application risk from vulnerabilities with limited or no applicable exposure.	RFP Requirement is applicable	10	Select	0	
27	The solution shall provide configurable application-security policies, rules, thresholds and organizational security requirements.	RFP Requirement is applicable	10	Select	0	
28	The solution shall support custom policies and rules to address Bank-specific application-security requirements.	RFP Requirement is applicable	10	Select	0	
29	The solution shall support exception and risk-acceptance management, including appropriate authorization, justification, validity period and auditability.	RFP Requirement is applicable	10	Select	0	
30	The solution shall provide guided, semi-automated and/or automated remediation capabilities for supported application-security findings.	RFP Requirement is applicable	10	Select	0	
31	The solution shall provide actionable remediation recommendations identifying the affected application/component, security issue, risk/severity, recommended corrective action and relevant security control, wherever applicable.	RFP Requirement is applicable	10	Select	0	
32	The solution shall support integration with the Bank's existing SIEM, SOAR, ITSM, SOC and security-management platforms through APIs, connectors, webhooks or equivalent mechanisms.	RFP Requirement is applicable	10	Select	0	
33	The solution shall provide centralized dashboards for application risk, vulnerable components, dependency risks, identity risks, attack paths, exposed applications, application relationships and remediation status.	RFP Requirement is applicable	10	Select	0	
34	The solution shall provide configurable reporting for CISO, management, application owners, developers, SOC and security teams, as applicable.	RFP Requirement is applicable	10	Select	0	

CNAPP						
S.No.	**Functional Specification**	**Updated in Addendum**	**Maximum Marks**	**Compliance (S/C)**	**Calculated Score**	**Remarks**
35	Reports shall provide, at minimum, application-security risk trends, critical findings, vulnerable components, application dependencies, high-risk identities, attack paths, remediation status and outstanding exceptions.	RFP Requirement is applicable	10	Select	0	
36	The solution shall support role-based access control (RBAC) with granular administrative permissions and segregation of duties.	RFP Requirement is applicable	10	Select	0	
37	The solution shall maintain an auditable history of relevant application-security findings, policy changes, configuration changes, remediation actions, exceptions and risk-acceptance activities.	RFP Requirement is applicable	10	Select	0	
38	The solution shall provide APIs or equivalent standard integration mechanisms for retrieving application inventory, application relationships, dependencies, vulnerabilities, risks, identity information, attack paths and remediation information, as applicable.	RFP Requirement is applicable	10	Select	0	
39	The solution shall support continuous or periodic reassessment of application security throughout the development, deployment and operational lifecycle, based on the capabilities supported by the proposed solution.	RFP Requirement is applicable	10	Select	0	
40	The solution shall provide mechanisms for tracking the security posture and risk of applications over their lifecycle, including newly identified vulnerabilities, changes in application dependencies, identity relationships and exposure.	RFP Requirement is applicable	10	Select	0	
41	The solution shall support tagging, metadata and/or equivalent mechanisms to associate applications with business units, application owners, environments, criticality and other Bank-defined attributes.	RFP Requirement is applicable	10	Select	0	
42	The solution shall provide search, filtering, drill-down and correlation capabilities across applications, components, dependencies, identities, vulnerabilities, attack paths and associated security findings.	RFP Requirement is applicable	10	Select	0	
43	The solution shall provide mechanisms to identify and track unmanaged, unknown or previously undiscovered application components and relationships, where such visibility is technically supported.	RFP Requirement is applicable	10	Select	0	
44	The solution shall support integration with external vulnerability, threat-intelligence and security-data sources, where required, to enhance application risk prioritization and contextual analysis.	RFP Requirement is applicable	10	Select	0	
45	The solution shall provide security findings with sufficient context to enable security teams to determine the affected application, affected component, associated risk, potential impact and recommended remediation.	RFP Requirement is applicable	10	Select	0	
46	The solution shall provide a unified application-centric risk view by correlating application components, dependencies, identities, permissions, APIs, cloud-native services and relevant security findings.	RFP Requirement is applicable	10	Select	0	
47	The proposed CNAPP solution shall provide the specified security capabilities through native functionality, integrated modules, supported connectors, APIs, application integrations or other functionally equivalent mechanisms.	RFP Requirement is applicable	10	Select	0	
48	Capabilities delivered through integrated modules or connectors shall be centrally manageable and correlated through the proposed CNAPP platform and shall provide a unified view of the applicable application-security risks.	RFP Requirement is applicable	10	Select	0	
49	A capability shall not be considered non-compliant solely because it is delivered through an integrated module, supported connector, API or security workflow, provided the bidder demonstrates that the required security outcome is achieved.	RFP Requirement is applicable	10	Select	0	
50	The bidder shall clearly identify, for every functional requirement, the product/module/component through which the capability is provided and shall specify any licensing, subscription, connector or integration dependency.	RFP Requirement is applicable	10	Select	0	
51	The proposed solution shall support secure integration with the Bank's existing security architecture and shall enable forwarding of relevant application-security findings, risk scores, vulnerabilities and associated metadata to the Bank's SOC/SIEM/SOAR platforms.	RFP Requirement is applicable	10	Select	0	

CNAPP						
S.No.	**Functional Specification**	**Updated in Addendum**	**Maximum Marks**	**Compliance (S/C)**	**Calculated Score**	**Remarks**
52	The solution shall support encryption of applicable security information and management communication in transit and at rest, in accordance with the Bank's security requirements and applicable deployment model.	RFP Requirement is applicable	10	Select	0	
53	The solution shall support secure authentication and authorization mechanisms for administrative and API access, including MFA and/or integration with enterprise identity services, wherever supported.	RFP Requirement is applicable	10	Select	0	
54	The solution shall provide mechanisms to protect application-security information against unauthorized access, modification or deletion through access controls, audit mechanisms and other appropriate security controls.	RFP Requirement is applicable	10	Select	0	
55	The solution shall support high availability and service continuity appropriate to the proposed deployment architecture and shall provide mechanisms for recovery of relevant configurations, policies and security information.	The solution shall support service continuity appropriate to the proposed deployment architecture and shall provide mechanisms for recovery of relevant configurations, policies and security information.	10	Select	0	
56	The solution shall provide a mechanism for identifying critical application-security risks requiring immediate attention, based on configurable severity and risk criteria.	RFP Requirement is applicable	10	Select	0	
TOTAL MARKS			**560**		**0**	

CWPP						
S.No.	**Functional Specification**	**Updated in Addendum**	**Maximum Marks**	**Compliance (S/C)**	**Calculated Score**	**Remarks**
The OEM shall submit mandatory compliance with the Cloud Deployment requirements along with the Functional Specifications of the proposed solution.						
1	The proposed Cloud Workload Protection Platform (CWPP) shall provide centralized capabilities for protecting, monitoring, detecting, investigating and responding to security threats affecting cloud workloads during runtime.	RFP Requirement is applicable	10	Select	0	
2	The solution shall support protection of workloads deployed across physical, virtual, private-cloud, public-cloud and hybrid-cloud environments, as applicable.	RFP Requirement is applicable	10	Select	0	
3	The solution shall support major public-cloud environments including AWS, Microsoft Azure and Google Cloud Platform, as applicable.	RFP Requirement is applicable	10	Select	0	
4	The solution shall provide visibility and protection for supported virtual machines, cloud instances, containers, Kubernetes workloads and other supported cloud workloads.	RFP Requirement is applicable	10	Select	0	
5	The solution shall automatically discover and maintain an inventory of onboarded/protected workloads, including workload type, operating system, environment and protection status.	RFP Requirement is applicable	10	Select	0	
6	The solution shall provide continuous or near-real-time monitoring of protected workloads for malicious activity, suspicious behavior, unauthorized changes and security threats.	RFP Requirement is applicable	10	Select	0	
7	The solution shall provide runtime threat detection and prevention capabilities for supported workloads.	RFP Requirement is applicable	10	Select	0	
8	The solution shall detect and prevent, where supported, malware, ransomware, trojans, rootkits and other malicious software or activities affecting protected workloads.	RFP Requirement is applicable	10	Select	0	
9	The solution shall monitor process execution and process behavior and identify suspicious, unauthorized or malicious processes.	RFP Requirement is applicable	10	Select	0	
10	The solution shall detect suspicious process chains, abnormal parent-child process relationships and other execution patterns indicative of compromise.	RFP Requirement is applicable	10	Select	0	
11	The solution shall monitor and detect suspicious command-line execution, scripts, interpreters and other execution mechanisms, as applicable to supported operating systems.	RFP Requirement is applicable	10	Select	0	
12	The solution shall detect suspicious use of legitimate system tools and utilities associated with Living-off-the-Land or equivalent attack techniques.	RFP Requirement is applicable	10	Select	0	
13	The solution shall provide behavioral and/or heuristic analysis to identify anomalous or previously unknown malicious activity affecting protected workloads.	RFP Requirement is applicable	10	Select	0	
14	The solution shall detect activities indicative of privilege escalation, persistence, lateral movement, credential misuse and other post-compromise techniques.	RFP Requirement is applicable	10	Select	0	
15	The solution shall monitor relevant network communications involving protected workloads and identify suspicious or unauthorized communication patterns.	RFP Requirement is applicable	10	Select	0	
16	The solution shall identify communication with known or suspected malicious infrastructure, including malicious IP addresses, domains, URLs, command-and-control infrastructure or equivalent threat indicators, where applicable.	RFP Requirement is applicable	10	Select	0	
17	The solution shall provide host/workload-based intrusion detection and/or prevention capabilities for supported operating systems and workloads.	RFP Requirement is applicable	10	Select	0	
18	The solution shall monitor critical files, directories, system objects and configuration elements for unauthorized modification, creation or deletion, where supported.	RFP Requirement is applicable	10	Select	0	
19	The solution shall provide file integrity monitoring for designated critical files, directories and system objects.	RFP Requirement is applicable	10	Select	0	
20	The solution shall detect suspicious creation or modification of system accounts, services, scheduled tasks and other persistence mechanisms, where applicable.	RFP Requirement is applicable	10	Select	0	
21	The solution shall provide protection against ransomware and destructive activities, including detection of abnormal file encryption or mass file modification behavior.	RFP Requirement is applicable	10	Select	0	
22	The solution shall provide exploit detection and/or prevention capabilities for supported workload operating systems and applications.	RFP Requirement is applicable	10	Select	0	
23	The solution shall support virtual patching or equivalent compensating protection mechanisms, where applicable, for vulnerabilities for which immediate patching is not feasible.	RFP Requirement is applicable	10	Select	0	

CWPP						
S.No.	Functional Specification	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
24	The solution shall support detection and/or prevention of web-shell and other unauthorized application-level persistence mechanisms, where applicable.	RFP Requirement is applicable	10	Select	0	
25	The solution shall provide runtime security monitoring and threat detection for containerized workloads, where supported.	RFP Requirement is applicable	10	Select	0	
26	The solution shall provide runtime protection for Kubernetes workloads, including supported pods, containers and workload processes.	RFP Requirement is applicable	10	Select	0	
27	The solution shall detect suspicious behavior involving containers, pods, workload processes and workload-to-workload communications, where applicable.	RFP Requirement is applicable	10	Select	0	
28	The solution shall provide security monitoring for serverless workloads/functions, where supported by the proposed solution and cloud platform.	RFP Requirement is applicable	10	Select	0	
29	The solution shall support agent-based and/or agentless protection mechanisms, as applicable to different workload types and supported environments.	RFP Requirement is applicable	10	Select	0	
30	Where an agent is required, the solution shall provide mechanisms for secure deployment, centralized management, health monitoring and controlled upgrade of the workload protection agent.	RFP Requirement is applicable	10	Select	0	
31	The solution shall support centralized security policies for different workload types, operating systems, applications, environments and business groups.	RFP Requirement is applicable	10	Select	0	
32	The solution shall support configurable response actions for detected threats, including alerting, blocking, process termination, file quarantine, workload isolation or other equivalent containment actions, as applicable.	RFP Requirement is applicable	10	Select	0	
33	The solution shall provide workload isolation or containment capabilities to limit the impact or spread of a confirmed or suspected compromise, where supported.	RFP Requirement is applicable	10	Select	0	
34	The solution shall provide security investigation capabilities using relevant process, file, network, user, workload and event-level information.	RFP Requirement is applicable	10	Select	0	
35	The solution shall provide historical workload activity and security-event information sufficient to support investigation and forensic analysis.	RFP Requirement is applicable	10	Select	0	
36	The solution shall provide process-tree or equivalent process-relationship visualization to assist in investigation of suspicious activity.	RFP Requirement is applicable	10	Select	0	
37	The solution shall support workload-level threat hunting using available security telemetry and configurable search criteria.	RFP Requirement is applicable	10	Select	0	
38	The solution shall support identification and searching of Indicators of Compromise (IoCs), including supported hashes, IP addresses, domains, URLs and equivalent indicators.	RFP Requirement is applicable	10	Select	0	
39	The solution shall support integration with external threat-intelligence sources to enhance workload threat detection and investigation.	RFP Requirement is applicable	10	Select	0	
40	The solution shall provide contextual security alerts containing relevant information such as affected workload, severity, detection type, process, user, file, network activity, timestamp and recommended response, as applicable.	RFP Requirement is applicable	10	Select	0	
41	The solution shall provide centralized dashboards and reporting covering workload inventory, security status, threats, incidents, policy violations, vulnerabilities exploited at runtime and response/containment status.	RFP Requirement is applicable	10	Select	0	
42	The solution shall support integration with the Bank's existing SIEM, SOAR, SOC and ITSM/security-management platforms through APIs, connectors, webhooks, syslog or equivalent mechanisms.	RFP Requirement is applicable	10	Select	0	
43	The solution shall support forwarding of relevant security events, alerts, incidents, risk information and associated metadata to the Bank's centralized SIEM/SOC platform.	RFP Requirement is applicable	10	Select	0	
44	The solution shall provide role-based access control (RBAC) with granular administrative permissions and support segregation of duties, as applicable.	RFP Requirement is applicable	10	Select	0	
45	The solution shall maintain an auditable record of administrative activities, policy changes, security events, response actions and other relevant security activities.	RFP Requirement is applicable	10	Select	0	
46	The solution shall provide secure authentication and authorization for administrative access, including MFA and/or integration with the Bank's enterprise identity service, as applicable.	RFP Requirement is applicable	10	Select	0	
47	The solution shall support high availability and service continuity appropriate to the proposed deployment architecture and shall provide mechanisms for recovery of relevant configurations and security policies.	The solution shall support service continuity appropriate to the proposed deployment architecture and shall provide mechanisms for recovery of relevant configurations and security policies.	10	Select	0	

CWPP						
S.No.	**Functional Specification**	**Updated in Addendum**	**Maximum Marks**	**Compliance (S/C)**	**Calculated Score**	**Remarks**
48	The solution shall provide mechanisms to identify the protection health/status of onboarded workloads, including agent, connector or communication health where applicable.	RFP Requirement is applicable	10	Select	0	
49	The solution shall support consumption and correlation of relevant vulnerability, SBOM, CBOM and threat-intelligence information from the Bank's separately procured security solutions through APIs, supported integrations or equivalent mechanisms, where technically supported.	RFP Requirement is applicable	10	Select	0	
50	The proposed CWPP shall provide the specified workload-protection capabilities through native functionality, integrated modules, supported agents, connectors, APIs or other functionally equivalent mechanisms. The bidder shall clearly identify the product/module through which each requirement is fulfilled and shall provide appropriate OEM documentation or demonstration as evidence of compliance.	RFP Requirement is applicable	10	Select	0	
TOTAL MARKS			**500**		**0**	

Continous Threat Exposure Management (CTEM)						
S.No.	Functional Specification	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
The OEM shall submit mandatory compliance with the Cloud Deployment requirements along with the Functional Specifications of the proposed solution.						
1	The solution should collect intelligence from multiple languages and relevant regional sources, with support for multilingual threat intelligence processing and analysis.	Clause Stands Deleted.				
2	The solution should support translation or interpretation of collected intelligence into English	Clause Stands Deleted.				
3	The solution should extract technical data from available intelligence sources	RFP Requirement is applicable	10	Select	0	
4	The solution shall utilize artificial intelligence, machine learning, analytics, human analyst validation, or equivalent mechanisms, as applicable, to identify, correlate and minimize false positives in threat intelligence and exposure findings.	RFP Requirement is applicable	10	Select	0	
5	The solution should provide automated and/or AI-assisted generation of tailored intelligence reports based on customer requirements	RFP Requirement is applicable	10	Select	0	
6	The solution should enrich intelligence results and filter by author, severity, source, date, asset association, and other criteria	RFP Requirement is applicable	10	Select	0	
7	Each intelligence item should include metadata such as date, author, source, and pre-classification of raw data	Each intelligence item should include metadata such as date, author, source etc.	10	Select	0	
8	The solution should allow messaging and collaboration within the context of a specific intelligence item	RFP Requirement is applicable	10	Select	0	
9	The solution shall provide access to proprietary, internally generated, licensed or equivalent high-quality threat intelligence sources capable of providing actionable intelligence relevant to the Bank's environment	RFP Requirement is applicable	10	Select	0	
10	Analysts should perform threat hunting activities to find findings outside of the platform	Clause Stands Deleted.				
11	The solution/service should generate investigation reports for designated VIPs or other high-risk identities/assets, providing an overview of identified digital exposure and associated risk.	RFP Requirement is applicable	10	Select	0	
12	The solution should provide general and industry-related cyber intelligence reports on threat landscape trends, at least twice a month	The Solution should provide general and industry-related cyber intelligence reports on threat landscape trends.	10	Select	0	
13	The solution should be able to commission ad-hoc research reports on demand	RFP Requirement is applicable	10	Select	0	
14	The solution should provide a graphical dashboard with views for alerts, reports, digital footprint, and raw intelligence	RFP Requirement is applicable	10	Select	0	
15	The solution should provide REST API integration with SIEM, SOAR, and ticketing systems	RFP Requirement is applicable	10	Select	0	
16	The solution should support IOC reputation queries via direct API	RFP Requirement is applicable	10	Select	0	
17	The solution should provide secure APIs and/or standard integration mechanisms to support integration with authorized AI, automation and security platforms.	RFP Requirement is applicable	10	Select	0	
18	The solution should provide comprehensive threat actor attribution including known identities, motivations, historical activity, TTPs, associated infrastructure, and MITRE ATT&CK mapping	The solution shall provide threat context for identified exposures, like associated threat actors/campaigns, observed exploitation activity, TTPs, MITRE ATT&CK mapping.	10	Select	0	
19	The solution should detect compromised credentials for employees and VIPs, exposed payment card information, and aggregate data from known breach databases in real time	Clause Stands Deleted.				
20	The solution should support IoC enrichment — allowing submission of IPs, domains, and hashes to receive contextual threat intelligence and threat actor attribution	Clause Stands Deleted.				
21	The solution should support threat actor interaction via vendor analysts (e.g., engaging via dark web avatars) to gather additional intelligence	Clause Stands Deleted.				
22	The solution should support scanning and reputation analysis of submitted IP addresses	Clause Stands Deleted.				
23	The solution should support reporting of confirmed malicious or phishing assets to relevant external platforms and authorities, where such reporting is supported and authorized.	Clause Stands Deleted.				
24	The solution should provide pre-built bidirectional integrations with SIEM, SOAR, ticketing (Manage Engine), and threat intelligence platforms	The solution should provide integrations with SIEM, SOAR, ticketing (Manage Engine), and threat intelligence platforms.	10	Select	0	

Continous Threat Exposure Management (CTEM)						
S.No.	Functional Specification	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
25	The solution should comply with regulatory and industry standards including PCI DSS, GDPR, ISO 27001, and SOC 2 Type II	RFP Requirement is applicable	10	Select	0	
26	The solution should continuously discover the digital presence, detect new assets, and present deltas of newly discovered assets without requiring the organization to provide asset information upfront	RFP Requirement is applicable	10	Select	0	
27	Asset discovery should include continuous or periodic discovery of internet-facing assets, including IP addresses, domains, sub-domains, certificates, cloud-exposed services and other publicly accessible digital assets	RFP Requirement is applicable	10	Select	0	
28	The solution should support ad-hoc scan and discovery of assets for any input domain	RFP Requirement is applicable	10	Select	0	
29	Each discovered asset should include parameters such as Asset, Asset Type, Discovery Reason, Issues, Created Date, and Status	RFP Requirement is applicable	10	Select	0	
30	The solution shall provide automated validation of identified exposures, where technically applicable and authorized by the Bank, using controlled, non-destructive testing or equivalent validation mechanisms to determine whether the identified exposure is genuinely exploitable or materially exposed.	The solution shall provide continuous assessment and validation of identified exposures using available security, vulnerability, configuration and exposure data to determine their materiality, reachability and potential exploitability, and shall support risk-based prioritization of such exposures.	10	Select	0	
31	The solution should display a Security Score overview with full breakdown by issue category	RFP Requirement is applicable	10	Select	0	
32	Issues to be sorted and filtered by severity level (Very High, High, Medium, Low, Info)	RFP Requirement is applicable	10	Select	0	
33	The solution should validate that a vulnerability is actually exploitable or otherwise materially exposed (active exposure validation)	Clause Stands Deleted.				
34	The solution should provide contextualized alerts and risk analysis based on identified assets, exposures, threat intelligence and available organizational context, using AI/ML or equivalent analytic	RFP Requirement is applicable	10	Select	0	
35	The solution should detect malicious files, reconnaissance activity, automated attack tools, and target lists	Clause Stands Deleted.				
36	Each discovered issue should include fields for Severity, Asset, Asset Status, Asset Type, First/Last Seen Date, and Issue Status	RFP Requirement is applicable	10	Select	0	
37	The solution should allow generation of an immediate report with full digital presence and issues list in PDF and CSV format	RFP Requirement is applicable	10	Select	0	
38	The solution should be deployed agentlessly, without requiring sensors or agents on endpoints, servers, or network appliances	The solution should be deployed agent/agentlessly, without requiring sensors or agents on endpoints, servers or network appliances.	10	Select	0	
39	The solution should integrate via APIs with the existing security stack including NGFW, WAF, XDR, and UEM platforms and other relevant security controls.	RFP Requirement is applicable	10	Select	0	
40	The solution should continuously or periodically identify vulnerabilities, misconfigurations and other exposure conditions across the Bank's internet-facing attack surface, including on-premises and cloud-hosted assets	RFP Requirement is applicable	10	Select	0	
41	The solution should support external vulnerability source integrations such as VA/VM scanners, ASM, XDR, BAS, Dark Web Monitoring, and MDM/UEM	RFP Requirement is applicable	10	Select	0	
42	The solution should use machine learning to evaluate the business impact of each remediation action and prioritize high-priority exposures	RFP Requirement is applicable	10	Select	0	
43	The ML model should continuously study the environment including asset relationships, topology, and security controls to detect false positives and identify root causes	RFP Requirement is applicable	10	Select	0	
44	The solution should identify false positives in vulnerability findings	RFP Requirement is applicable	10	Select	0	
45	The solution should support manual IoC management operations	Clause Stands Deleted.				
46	The solution should support ingestion of IOC, threat intelligence and external exposure data from configurable third-party and/or bank-approved sources through supported integration mechanisms.	RFP Requirement is applicable	10	Select	0	
47	The solution should support cross-platform IoC enforcement across the security stack	Clause Stands Deleted.				
48	The solution should assess and harden network, endpoint, and operating system security controls	Clause Stands Deleted.				

Continous Threat Exposure Management (CTEM)						
S.No.	Functional Specification	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
49	The solution should provide a private exposure map of the organization's attack surface	The solution should provide an organization-specific view of the Bank's attack surface, identified exposures, vulnerabilities, misconfigurations etc.	10	Select	0	
50	The solution should support custom protections tailored to the organization's environment	RFP Requirement is applicable	10	Select	0	
51	The solution should apply virtual patching/compensating controls/exposure mitigation mechaism to the firewall and other security systems through integration with relevant security controls.	The CTEM solution shall identify, prioritize and recommend applicable virtual patching, compensating controls and exposure-mitigation mechanisms, and shall support integration with relevant security controls for remediation or mitigation, including through approved workflows or automation	10	Select	0	
52	Each alert should provide targeted info, actionable description, evidence, and clear remediation steps	RFP Requirement is applicable	10	Select	0	
53	Each alert should include a discussion board for eligible users to collaborate within the alert context	RFP Requirement is applicable	10	Select	0	
54	The solution should support role-based access for viewing and receiving notifications for all or specific alerts	RFP Requirement is applicable	10	Select	0	
55	The solution should include IOC investigation, infrastructure mapping, and threat actor identification	RFP Requirement is applicable	10	Select	0	
56	The visual investigation tool should integrate multiple services including WHO IS and Passive DNS	RFP Requirement is applicable	10	Select	0	
57	Up on demand, the vendor should provide a dedicated Customer Success Manager as a single point of contact for onboarding and ongoing support	RFP Requirement is applicable	10	Select	0	
58	The vendor to provide 24/7 system support	RFP Requirement is applicable	10	Select	0	
59	The solution should support API-based remediation, notification or workflow integration with relevant security controls	The CTEM solution shall provide API/webhook-based capabilities for remediation, notification or workflow integration with relevant security controls.	10	Select	0	
60	The solution should support automated remediation workflows	The CTEM solution shall support integration and workflow orchestration for automated remediation workflows.	10	Select	0	
61	The solution should ensure remediation actions do not disrupt business continuity	RFP Requirement is applicable	10	Select	0	
62	The solution should leverage compensating controls and layered defense strategies to manage threats proactively	Clause Stands Deleted.				
63	The solution should provide collaboration tools and ITSM integration for remediation workflows	RFP Requirement is applicable	10	Select	0	
64	The solution should analyze and enrich attack intelligence across the entire security stack	RFP Requirement is applicable	10	Select	0	
65	The solution should aim to reduce Mean Time to Remediate (MTTR) and labor costs	The CTEM solution shall provide capabilities to measure, monitor and report Mean Time to Remediate (MTTR) for identified exposures, including exposure ageing and remediation-status tracking.	10	Select	0	
66	The solution should maximize ROI from existing security tools by optimizing the security posture	The CTEM solution shall provide visibility and reporting on the coverage and effectiveness of existing security controls relevant to identified exposures.	10	Select	0	
67	The vendor to provide a mechanism to report security incidents identified through the platform and receive prompt response and guidance from the incident response team	The solution should have capability to report security incidents/alerts identified through the platform and collaborate with SOC team for prompt response and guidance.	10	Select	0	
68	The solution should support MFA for administrative access, role-based access control, and SSO integration	RFP Requirement is applicable	10	Select	0	
69	The solution should maintain detailed audit logs of user activity, administrative actions, and access attempts	RFP Requirement is applicable	10	Select	0	
TOTAL MARKS			550		0	

SIEM						
S.No.	Functional Specification	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
The OEM shall submit mandatory compliance with the Cloud Deployment						
1	The proposed solution must include Next Gen SIEM with necessary automation capabilities.	RFP Requirement is applicable	10	Select	0	
2	Proposed solution must provide unified dashboard.	RFP Requirement is applicable	10	Select	0	
3	The proposed SIEM solution should support logical segregation and management of different data sets based on organizational requirements. The solution should provide capabilities to define appropriate data access, search, and retention policies for different categories of security data.	RFP Requirement is applicable	10	Select	0	
4	The proposed solution should support ingestion and processing of structured and unstructured data from various sources. The solution should be capable of handling data irrespective of predefined schema or format changes and should ensure that collected events are retained without loss. The solution should provide the capability to utilize raw or unparsed data for search, correlation, analytics, and machine learning-based analysis.	RFP Requirement is applicable	10	Select	0	
5	The proposed SIEM solution shall provide embedded AI/ML-driven analytics for behavioral analysis, anomaly detection, risk scoring, threat correlation, predictive analytics, and automated prioritization of security events. The solution shall support AI/ML-assisted threat hunting, investigation, and timeline reconstruction, while providing an extensible framework for integration with external ML frameworks or custom analytics through standard APIs or SDKs.	RFP Requirement is applicable	10	Select	0	
6	The proposed solution shall support dynamic log parsing and normalization upon ingestion. In cases where historical security telemetry must be re-parsed, re-processed, or re-modeled using updated parsing rules or processing logic, the platform shall provide high-speed, cloud-native mechanisms to re-process retained historical telemetry using the updated parsing and processing logic, without impacting active SOC performance, availability, or operational detection capabilities.	RFP Requirement is applicable	10	Select	0	
7	The proposed SIEM solution shall provide out-of-the-box capabilities to assess data coverage for MITRE ATT&CK techniques and sub-techniques, identify telemetry or data gaps, and recommend the required log sources or data sources to improve detection coverage across the MITRE ATT&CK framework and Cyber Kill Chain.	RFP Requirement is applicable	10	Select	0	
8	Log Filtering – Not all logs are needed for the compliance requirements faced by organization, or for forensic purposes. Logs can be filtered by the source system, times, or by other rules defined by the SIEM administrator.	RFP Requirement is applicable	10	Select	0	
9	SIEM solution must **Integrate with external** threat intelligence to enrich/correlate events collected and should support integration with Opensource/3rd party TI feeds as well.	RFP Requirement is applicable	10	Select	0	
10	SIEM solution should be based on open architecture so that it can be used to feed data to 3rd party analytic solutions i.e. Solution should support standard CEF or equivalent technology which is accepted globally not the proprietary one.	RFP Requirement is applicable	10	Select	0	
11	The solution must ensure all the system components continue to operate in case of any other part of the system fails or loses connectivity.	RFP Requirement is applicable	10	Select	0	
12	The proposed solution should have physical or logical separation of the collection module, logging module and analysis / correlation module with the ability for adding more devices, locations, applications, etc.	RFP Requirement is applicable	10	Select	0	
13	The proposed solution must support caching mode of transfer for data collection, to ensure data is being logged in the event of loss of network connectivity, and resume sending of data upon network connection.	RFP Requirement is applicable	10	Select	0	
14	The proposed solution must have a user-friendly interface to convert statistical results to dashboard. The Dashboard should be accessible from the endpoints as & when required.	RFP Requirement is applicable	10	Select	0	

SIEM						
S.No.	**Functional Specification**	**Updated in Addendum**	**Maximum Marks**	**Compliance (S/C)**	**Calculated Score**	**Remarks**
15	The Proposed solution must offer all the below built-in threat detection techniques out of the box or through customization but should be availbale on day 1 : -	RFP Requirement is applicable	-	-	-	
15.1	• File reputation	RFP Requirement is applicable	10	Select	0	
15.2	Detect APT Threats	RFP Requirement is applicable	10	Select	0	
15.3	Integrate with any Honeypot/Deception solutions	RFP Requirement is applicable	10	Select	0	
15.4	Integrate with any NDR/XDR tools	RFP Requirement is applicable	10	Select	0	
15.5	Detect threats indicated by advisories	RFP Requirement is applicable	10	Select	0	
15.6	Give visibility of endpoints also by integrating with XDR, Antivirus etc. for endpoint analytics.	RFP Requirement is applicable	10	Select	0	
16	The proposed SIEM solution shall support reusable search or query logic that can be centrally defined and reused across searches, dashboards, reports, alerts, analytics, correlation rules, and other supported functions	RFP Requirement is applicable	10	Select	0	
17	The proposed solution shall be scalable and shall provide a cloud-native, highly available architecture with built-in redundancy and service continuity. The solution shall provide continuous security monitoring through cloud-native high availability and disaster recovery capabilities, with a minimum uptime commitment of 99.9%	RFP Requirement is applicable	10	Select	0	
18	The proposed solution shall provide cloud-native high availability and redundancy mechanisms to tolerate failures of underlying infrastructure components without disruption to security monitoring and operational capabilities. The solution shall provide automated failover and service continuity within the cloud environment through the CSP's native availability and resiliency capabilities	The proposed solution shall provide cloud-native high availability and redundancy mechanisms to tolerate failures of underlying infrastructure components without disruption to security monitoring and operational capabilities. The solution shall provide automated failover and service continuity.	10	Select	0	
19	The proposed solution must support caching mode of transfer for data collection, to ensure data is being logged in the event of loss of network connectivity, and resume sending of data upon network connection.	RFP Requirement is applicable	10	Select	0	
20	The proposed SIEM solution shall provide an integrated interface or equivalent mechanism to create, test, validate, and manage log parsers. The solution shall support validation of parsing configurations using live or historical data without impacting production data ingestion, processing, or security monitoring operations	RFP Requirement is applicable	10	Select	0	
21	Solution must be **agent based/agent less**	RFP Requirement is applicable	10	Select	0	
22	SIEM solution must support Out of the box integration with well known technologies e.g. firewall, AD, Switches, routers, Threat Intelligence etc. for creating response to an incidence	RFP Requirement is applicable	10	Select	0	
23	Where a native parser or connector is unavailable, the proposed solution shall provide supported mechanisms, SDKs, APIs, templates, or configuration interfaces to develop and maintain custom integrations	RFP Requirement is applicable	10	Select	0	
24	The proposed solution shall provide visibility and manageability of data parsing configurations through supported mechanisms. The solution shall allow authorized administrators to create, modify, and customize parsing or normalization rules as required for security monitoring and operational requirements without impacting existing data collection and processing.	RFP Requirement is applicable	10	Select	0	
25	All logs should be Authenticated (time-stamped), encrypted OR transmitted over a secure encrypted channel and compressed before / after transmission. No performance deggration should happen	RFP Requirement is applicable	10	Select	0	
26	The solution should have the capability to compress the logs for storage optimization.	RFP Requirement is applicable	10	Select	0	
27	The proposed solution should have capability to provide centrally or remotely log collector installation to integrate event sources. This is to ensure to reduce time of implementation as well as any changes to be made later through single click push from central site.	RFP Requirement is applicable	10	Select	0	
28	Caching & Batching: The proposed solution must support local caching and batching at collection level in case of connectivity failures.	RFP Requirement is applicable	10	Select	0	

SIEM						
S.No.	**Functional Specification**	**Updated in Addendum**	**Maximum Marks**	**Compliance (S/C)**	**Calculated Score**	**Remarks**
29	In case the connectivity with SIEM management system is lost, the collector should be able to store the data in its own repository. The retention, deletion, synchronization with SIEM database should be automatic.	RFP Requirement is applicable	10	Select	0	
30	Any failures of the event collection infrastructure must be detected and operations personnel must be notified as per SLA. The device Health monitoring must include the ability to validate that original event sources are still sending events	RFP Requirement is applicable	10	Select	0	
31	The solution should be able to store both normalized and RAW logs. Solution must support searching, Analytics and reporting of logs.	RFP Requirement is applicable	10	Select	0	
	Supported Data Sources					
32	The proposed solution must be able to support both real-time and on-demand access to data sources from files, network ports, database connections, custom APIs and interfaced incl. text, XML, JSON and other evolving format.	RFP Requirement is applicable	10	Select	0	
33	The proposed solution must be able to read data input from the following log file formats:					
33.1	Archived Log Files (Single line, Multi-line, and Complex XML and JSON Structure)	RFP Requirement is applicable	10	Select	0	
33.2	Windows Events Logs	RFP Requirement is applicable	10	Select	0	
33.3	Standard Log Files from applications such as Web (HTTP) servers, FTP servers, Email (SMTP/Exchange) servers, DNS servers, DHCP servers, Active Directory servers, etc.	RFP Requirement is applicable	10	Select	0	
34	The proposed solution must be able to accept the following indicative live data streams feeding through the network:	RFP Requirement is applicable	-	-	-	
34.1	Syslog Messages	RFP Requirement is applicable	10	Select	0	
34.2	Security Alerts	RFP Requirement is applicable	10	Select	0	
34.3	JSON streaming over HTTP/HTTPS	RFP Requirement is applicable	10	Select	0	
35	The proposed solution must support the decoding of the following indicative network protocols from log data or picking the meta data from network traffic: HTTP, FTP, DNS, MySQL, SMTP, SNMP, SMB, TCP, UDP, NFS, Oracle (TNS), LDAP/AD, PostgreSQL, Sybase/SQL Server (TDS), IMAP, POP3, RADIUS, IRC, SIP, DHCP, AMQP, DIAMETER, MAPI	RFP Requirement is applicable	10	Select	0	
36	The proposed solution must come with out-of the-box/customied to be delivered on day 1 support integration and dashboards, reports, rules etc. to provides rapid insights and operational visibility into large-scale CentOS, Windows, Unix and Linux environments machine data.: syslog, metrics and configuration files.	RFP Requirement is applicable	10	Select	0	
37	Events should be presented in a manner that is independent of device specific syntax and easy to understand for all users	RFP Requirement is applicable	10	Select	0	
38	Solution should have the ability to perform free text searches for events, incidents, rules and other parameters.	RFP Requirement is applicable	10	Select	0	
39	Proposed solution should support searching of Data/artifacts associated with historical incidents.	RFP Requirement is applicable	10	Select	0	
40	The solution should have the capability to identify / remember frequently used queries	RFP Requirement is applicable	10	Select	0	
	Index, Search, Filter, Analyze and Investigate					
41	The proposed SIEM solution shall ingest, index, and analyze structured and unstructured telemetry from applications, servers, databases, cloud services, network and security devices, including logs, events, configurations, messages, traps, alerts, metrics, and performance data through native, standards-based, or extensible data ingestion mechanisms, providing end-to-end visibility	RFP Requirement is applicable	10	Select	0	

SIEM						
S.No.	**Functional Specification**	**Updated in Addendum**	**Maximum Marks**	**Compliance (S/C)**	**Calculated Score**	**Remarks**
42	The proposed solution licensing shall be based on the volume of processed/ingested security data after applying applicable filtering, aggregation, or exclusion mechanisms. Events/logs filtered out before processing shall not be considered for license consumption. The licensing model shall align with the actual security data being monitored, processed, and retained by the Bank.	RFP Requirement is applicable	10	Select	0	
43	The proposed solution will be continuously used in the SOC so that solution builds specific repository which includes categories like including event types, tags, lookups, parsing/normalizing, actions and saved searches etc. It should help to discover and analyze various aspects in data. For example, event types should enable analyst to quickly classify and group similar events; then use to perform analytics on events.	RFP Requirement is applicable	10	Select	0	
44	SIEM solution must support API integration with 3rd party solutions.	RFP Requirement is applicable	10	Select	0	
	Monitor, Alert and Reporting Functions					
45	The proposed solution must be able to run any search on a schedule and set alerting conditions based on thresholds and deltas in the number and distribution of results across a time range or days like a histogram visualization.	RFP Requirement is applicable	10	Select	0	
46	The proposed solution must be able to execute automated corrective or follow-on actions via scripted alerts.	RFP Requirement is applicable	10	Select	0	
47	The proposed cloud-based solution shall support flexible data representation and analysis by enabling multiple views, schema interpretations, and query-time transformations of the same collected data without requiring redundant data storage or unnecessary reprocessing. The cloud platform shall support creation of customized searches, dashboards, and reports based on business and security monitoring requirements.	RFP Requirement is applicable	10	Select	0	
48	The proposed solution must be able to support sophisticated statistical and summary analysis by pipelining advanced search commands together in a single search.	RFP Requirement is applicable	10	Select	0	
49	The proposed solution must support the ability to perform calculations across various modules such as search, reporting, alerting, and dashboards	RFP Requirement is applicable	10	Select	0	
50	The proposed solution shall support AI/ML-based predictive analytics capabilities to analyze historical security data, alerts, and events for identifying emerging attack patterns, abnormal behaviors, and potential threats. The solution shall support correlation of multiple data attributes to provide proactive threat detection and investigation insights.	RFP Requirement is applicable	10	Select	0	
51	The proposed solution shall provide predictive analytics, anomaly detection, statistical analytics, or AI/ML-based analytical capabilities using:	RFP Requirement is applicable	-	-	-	
51.1	Uses historical data as a baseline to forecast future patterns, thresholds and tolerances	RFP Requirement is applicable	10	Select	0	
52	The proposed solution must come with prepackaged alerting capability, flexible service-based hosts grouping, and easy management of many data sources, and provide analytics ability to quickly identify bottlenecks and outliers.	RFP Requirement is applicable	10	Select	0	
53	The proposed solution should give visualization through a dashboard customizable to service groupings to help analyst.	RFP Requirement is applicable	10	Select	0	
54	The proposed solution should have the capability to collaborate and orchestrate with 3rd party solutions	RFP Requirement is applicable	10	Select	0	
55	The solution should be able to assign risk score with Scoring for various identified entities like user & assets should be possible based on the threats or correlations that particular host, username, entity, location has contributed. Indicative Use Case: Risk Score of User or Entity in the organization is calculated to reduce false positives and identify critical incidents by assigning the risk score of each and every subsequent offence and calculating the overall risk score based on the offens	RFP Requirement is applicable	10	Select	0	

SIEM						
S.No.	**Functional Specification**	**Updated in Addendum**	**Maximum Marks**	**Compliance (S/C)**	**Calculated Score**	**Remarks**
56	The solution must be able to provide a built-in facility to centralize incident analysis of entities in one location.	RFP Requirement is applicable	10	Select	0	
	Machine Learning					
57	The proposed solution shall provide a graphical interface or equivalent mechanism for configuring and managing pre-built or custom AI/ML analytics. The platform shall support integration with industry-standard machine learning frameworks, data science tools, and scripting languages through standard APIs, SDKs, or open interfaces.	RFP Requirement is applicable	10	Select	0	
58	The proposed solution machine learning capabilities must include API access, role- based access controls. for machine learning models.	RFP Requirement is applicable	10	Select	0	
59	The proposed solution machine learning capabilities must allow addition or have inbuild feature of custom machine learning algorithms from popular open-source libraries like NLP, Python etc.	RFP Requirement is applicable	10	Select	0	
60	The proposed solution shall provide integrated AI/ML capabilities as part of the proposed solution for security analytics, behavioral analytics, anomaly detection, threat detection, and risk-based analysis. The AI/ML capabilities shall be available without requiring the Bank to procure or deploy any separate third-party AI/ML platform to utilize the proposed functionality.	RFP Requirement is applicable	10	Select	0	
61	The proposed solution shall support real-time monitoring, collection, correlation, and alerting of Active Directory and identity-related security events through native capabilities or integration with supported identity, directory, endpoint, or operating system telemetry sources. The solution shall detect and generate alerts for security-relevant changes, including but not limited to users, groups, organizational units, policies, privileges, authentication events, and directory configurations to support security monitoring and investigation.	RFP Requirement is applicable	10	Select	0	
62	The proposed solution shall support monitoring, collection, correlation, and alerting of Windows operating system security events through native capabilities or integration with supported endpoint, operating system, or security monitoring solutions. The solution shall detect and generate alerts for security-relevant events including, but not limited to, file integrity, file systems, file shares, users and groups, processes, services, registry, removable media, scheduled tasks, privilege changes, configuration changes, and other Windows security events. The detected events shall support centralized monitoring, correlation, investigation, and incident response.	RFP Requirement is applicable	10	Select	0	
63	The proposed solution shall support monitoring, collection, correlation, and alerting of Linux/Unix operating system security events through native capabilities or integration with supported endpoint, operating system, or security monitoring solutions. The solution shall detect and generate alerts for security-relevant events including, but not limited to, file integrity, local and network file systems, users and groups, processes and daemons, mounted file systems, scheduled tasks, configuration files, privilege changes, service changes, and other Linux/Unix security events. The detected events shall support centralized monitoring, correlation, investigation, and incident response.	RFP Requirement is applicable	10	Select	0	
64	The system/solution should have the ability to correlate all the fields in a log					
64.1	IP	RFP Requirement is applicable	10	Select	0	
64.2	Domain	RFP Requirement is applicable	10	Select	0	
64.3	Endpoint	RFP Requirement is applicable	10	Select	0	
64.4	File Hash, Name, Extension, Path and Size	RFP Requirement is applicable	10	Select	0	
64.5	Registry Hive, Path, Key Name, Value Name, Value Type, Value Text, Value Data	RFP Requirement is applicable	10	Select	0	
64.6	Process Name, Arguments, Handle Name, Handle Type	RFP Requirement is applicable	10	Select	0	
64.7	Service Name, Description	RFP Requirement is applicable	10	Select	0	
64.8	Certificate	RFP Requirement is applicable	10	Select	0	

SIEM						
S.No.	**Functional Specification**	**Updated in Addendum**	**Maximum Marks**	**Compliance (S/C)**	**Calculated Score**	**Remarks**
64.9	Certificate Alias, Serial, Issuer, Subject, Start Time, End Time, Version, Handshake Type, Public key Algorithm, Signature Algorithm	RFP Requirement is applicable	10	Select	0	
64.10	Email	RFP Requirement is applicable	10	Select	0	
64.11	Email Address, Subject Body	RFP Requirement is applicable	10	Select	0	
65	The solution should allow the Bank to create its own use cases.	RFP Requirement is applicable	10	Select	0	
66	The solution should be able to integrate, automate and correlate with internal "Log sources" data sources to decide which threat to internal assets can be blocked with a high level of certainty/risk scoring.	RFP Requirement is applicable	10	Select	0	
67	The proposed solution shall provide advanced correlation capabilities either natively or through tightly integrated OEM components included in the proposed solution without requiring any third-party products.	RFP Requirement is applicable	10	Select	0	
68	Basic Statistical analysis that can be applied to any fields like calculating the length of command line arguments, HTTP user agent string, sub domains, URLs, standard deviation of count of events over time	RFP Requirement is applicable	10	Select	0	
69	The proposed solutions should use multiple technologies like using distance formula, geo Database, etc. to detect geographically improbable access	RFP Requirement is applicable	10	Select	0	
70	The proposed solution shall support advanced statistical, behavioral, or machine learning–based analytics to identify relationships, correlations, dependencies, or anomalies across multiple data fields. The solution shall enable analysts to derive contextual insights, improve threat detection, and support predictive security analytics based on patterns observed within historical and real-time security data.	RFP Requirement is applicable	10	Select	0	
71	The proposed solution's detection use cases should be comprised of guidance that provides an assessment of the Security Threat and how it helps detect and investigate it using the proposed solution. In addition, it should provide a summary of how the attack or detection technique maps to the following: MITRE ATTACK , an adversary behavior model that describes the actions an adversary might take.	RFP Requirement is applicable	10	Select	0	
72	Kill-Chain, a model that identifies the phases an adversary must complete to achieve their objective.	RFP Requirement is applicable	10	Select	0	
73	The proposed solution should also guide administrator on data sources required to implement detection technique from the same console (eg MITRE ATTACK)	RFP Requirement is applicable	10	Select	0	
74	The proposed solution must be able to run any search and set alerting conditions based on thresholds and deltas in the number and distribution of results across a time range or days like a histogram visualization.	RFP Requirement is applicable	10	Select	0	
75	The proposed solution must be able to execute automated corrective or follow-on actions via scripted alerts.	RFP Requirement is applicable	10	Select	0	
76	The proposed solution must have search criteria to be saved as dashboard or reports.	RFP Requirement is applicable	10	Select	0	
77	The proposed solution shall support graphical visualization of security events through configurable dashboards, timelines, and geographic and/or logical topology-based visualizations for enhanced monitoring and investigation.	RFP Requirement is applicable	10	Select	0	
78	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	RFP Requirement is applicable	10	Select	0	
79	The solution should provide a dashboard to display all the real-time events with drill-down functionality .	RFP Requirement is applicable	10	Select	0	
80	The solution must provide different role-based, user-based views to the dashboards which can be customized as per the requirements	RFP Requirement is applicable	10	Select	0	

SIEM						
S.No.	**Functional Specification**	**Updated in Addendum**	**Maximum Marks**	**Compliance (S/C)**	**Calculated Score**	**Remarks**
81	The solution should include reports directly aligned to support auditing/compliance requirements.	RFP Requirement is applicable	10	Select	0	
	Incident Response					
82	The proposed solution must provide investigation/ auditing capability to enable analysts to easily: Track searches and activities Review activities at any point Select and place into timeline for temporal analysis Help remember searches, steps taken, provide annotation support	RFP Requirement is applicable	10	Select	0	
83	The solution must be able to provide a built-in facility to centralize incident analysis of entities in one location.	RFP Requirement is applicable	10	Select	0	
84	The proposed solution should be able to trigger actions. These actions can be automatically triggered by correlation alerts or offences or manually run on an ad hoc basis from the Incident.	RFP Requirement is applicable	10	Select	0	
85	The proposed solution shall support out-of-the-box or standards-based integration with major commercially available SOAR platforms and security ecosystem solutions to enable automated response and orchestration.	RFP Requirement is applicable	10	Select	0	
86	The proposed solution should be **bidirectional** integrated with SOAR solution.	RFP Requirement is applicable	10	Select	0	
87	The proposed solution shall provide built-in investigation guidance, contextual recommendations, or equivalent analyst assistance capabilities to support the investigation, containment, eradication, and recovery of security incidents. The solution shall assist analysts with recommended response actions, investigation workflows, and relevant contextual information to improve the consistency, accuracy, and efficiency of incident response.	RFP Requirement is applicable	10	Select	0	
88	The proposed solutions.each components viz. SIEM, UEBA, & SOAR should have seamless bi-directional integrations.Also, the solution should provide the capability for unified console from where all the components can be monitored.	RFP Requirement is applicable	10	Select	0	
89	SIEM solution must provide built in **or it should be able to integrate with 3rd party ticketing tools** ticketing system to track incident from creation to closure, provide reports on pending incidents and permit upload of related evidences such as screenshots etc at the Incident management tool manually.	RFP Requirement is applicable	10	Select	0	
90	The solution should offer a means of escalating alerts between various users of the solution, such that if alerts are not acknowledged in a predetermined timeframe, that alert is escalated to ensure it is investigated.	RFP Requirement is applicable	10	Select	0	
91	The solution should include reports directly aligned to support auditing/compliance requirements.	RFP Requirement is applicable	10	Select	0	
92	The solution must automate internal health checks and notify the user in case of problems	RFP Requirement is applicable	10	Select	0	
93	The proposed solution shall include all licenses required to utilize the forensic investigation, threat hunting, incident investigation, and evidence analysis capabilities of the proposed solution from Day 1 of implementation. No additional licenses shall be required during the contract period to use the features	RFP Requirement is applicable	10	Select	0	
94	The proposed solution shall provide integrated AI/Generative AI capabilities to assist SOC analysts with alert investigation, incident summarization, threat hunting, evidence analysis and security query generation.	RFP Requirement is applicable	10	Select	0	
95	The solution shall support natural-language interaction for supported SOC operations, including security-data querying, investigation, incident summarization and explanation of security findings.	RFP Requirement is applicable	10	Select	0	
96	The solution shall provide AI-driven correlation and prioritization of security alerts and related events across available endpoint, network, identity and threat-intelligence telemetry.	RFP Requirement is applicable	10	Select	0	

SIEM						
S.No.	Functional Specification	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
97	The solution shall provide AI-assisted incident investigation, including identification of related entities, indicators, events and relevant historical security activity.	RFP Requirement is applicable	10	Select	0	
98	The solution shall provide AI-assisted threat hunting capabilities, including natural-language hunting, query generation and analysis of identified results.	RFP Requirement is applicable	10	Select	0	
99	The solution shall support AI-assisted detection engineering, including recommendation or generation of detection logic and security queries, subject to authorized analyst review.	RFP Requirement is applicable	10	Select	0	
100	The solution shall provide threat-intelligence enrichment of security alerts and investigations using available Networks and supported external intelligence sources.	RFP Requirement is applicable	10	Select	0	
101	The solution shall provide automated or analyst-approved response orchestration through Networks security controls and supported third-party security products.	RFP Requirement is applicable	10	Select	0	
102	The solution shall support automated response actions such as endpoint isolation, indicator blocking, account-related actions and other supported containment measures, subject to configured authorization policies.	RFP Requirement is applicable	10	Select	0	
103	The solution shall provide configurable human-in-the-loop controls for response actions requiring analyst review or approval.	RFP Requirement is applicable	10	Select	0	
104	The solution shall provide configurable RBAC and least-privilege controls governing access to security data, investigation capabilities, automation and response functions.	RFP Requirement is applicable	10	Select	0	
105	AI-driven and automated workflows shall operate only against authorized data sources, integrations, APIs and security controls configured by the Bank.	RFP Requirement is applicable	10	Select	0	
106	The solution shall provide risk- and policy-based controls to govern automated actions based on factors such as alert severity, confidence, asset criticality, user role and action type.	RFP Requirement is applicable	10	Select	0	
107	AI-generated findings and recommendations shall, wherever technically supported, provide supporting context and traceability to relevant security events, alerts, entities, indicators or telemetry.	RFP Requirement is applicable	10	Select	0	
108	The solution shall maintain audit records of AI-assisted investigations and automated activities, including relevant actions, recommendations, approvals and response execution details.	RFP Requirement is applicable	10	Select	0	
109	The proposed solution shall provide centralized incident context and attack-story correlation, enabling analysts to understand relationships between alerts, endpoints, users, applications, network activity and indicators.	RFP Requirement is applicable	10	Select	0	
110	The solution shall support integration and orchestration with Networks security technologies and supported third-party platforms, including EDR/XDR, firewalls, SOAR, IAM/PAM, email security, vulnerability management and threat intelligence.	RFP Requirement is applicable	10	Select	0	
111	The proposed cloud-delivered solution shall provide appropriate encryption, tenant isolation, secure authentication, MFA, RBAC, audit logging and protection of Bank security data in accordance with the applicable service architecture and SLA.	RFP Requirement is applicable	10	Select	0	
112	The bidder shall identify all products/modules, licenses, subscriptions and third-party dependencies required to deliver the proposed AI, investigation, automation, orchestration and response capabilities.	RFP Requirement is applicable	10	Select	0	
113	All mandatory capabilities proposed under the solution shall be generally available and operational from Day 1 of production implementation.	RFP Requirement is applicable	10	Select	0	
114	The proposed SIEM/NG-SIEM solution shall provide integrated AI-driven security operations capabilities to assist SOC analysts with alert triage, incident investigation, incident summarization, threat hunting, evidence analysis, root-cause analysis and generation of security queries and recommended investigation actions.	RFP Requirement is applicable	10	Select	0	

SIEM						
S.No.	Functional Specification	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
115	The solution shall support natural-language interaction for SOC operations, enabling authorized analysts to query security data, investigate incidents, obtain contextual explanations of security findings and initiate supported investigation or response workflows through natural-language interactions.	RFP Requirement is applicable	10	Select	0	
116	The solution shall provide AI/ML-driven correlation, analytics and prioritization of security events and alerts across multiple telemetry sources, including endpoint, network, cloud, identity, application and threat-intelligence data, and shall automatically group related alerts and events into meaningful security incidents wherever correlation is supported.	RFP Requirement is applicable	10	Select	0	
117	The solution shall provide AI-assisted incident investigation by automatically correlating relevant entities, indicators, events, telemetry and historical security activity and shall present an enriched incident timeline and attack story, including relevant causal relationships and supporting context, to enable rapid determination of root cause and impact.	RFP Requirement is applicable	10	Select	0	
118	The solution shall provide AI-assisted threat hunting capabilities, including natural-language threat hunting, automatic or assisted generation of security queries, analysis of hunting results and guided investigation of identified threats across available security telemetry.	RFP Requirement is applicable	10	Select	0	
119	The solution shall support AI-assisted detection engineering, including generation or recommendation of detection logic, queries, analytics and investigation content based on observed threats, security telemetry and relevant threat intelligence, with appropriate analyst validation and approval before production deployment where applicable.	RFP Requirement is applicable	10	Select	0	
120	The solution shall provide integrated threat-intelligence enrichment of security events, alerts and investigations using continuously updated threat intelligence and supported internal and external intelligence sources, and shall correlate relevant indicators with observed security activity to improve detection, prioritization and investigation.	RFP Requirement is applicable	10	Select	0	
121	The solution shall provide integrated security orchestration and automated response capabilities, enabling automated or analyst-approved execution of response workflows across the SIEM and connected security controls, including supported native and third-party security technologies.	RFP Requirement is applicable	10	Select	0	
122	The solution shall support automated or analyst-approved response actions, including endpoint containment, indicator blocking, account-related actions, network security control actions and other supported containment or remediation measures, based on detected threats, configured policies and available integrations.	RFP Requirement is applicable	10	Select	0	
123	The solution shall provide configurable human-in-the-loop controls for security response and automation, including analyst review, approval, rejection, modification or escalation of actions according to defined operational and security policies.	RFP Requirement is applicable	10	Select	0	
124	The solution shall provide granular role-based access control (RBAC) and least-privilege controls for security data, investigation, threat hunting, analytics, automation, orchestration and response functions, with segregation of duties where required by the Bank.	RFP Requirement is applicable	10	Select	0	
125	AI-driven analytics, automated workflows and response actions shall operate only against security data sources, integrations, APIs and security controls authorized and configured by the Bank, with appropriate access-control and governance mechanisms.	RFP Requirement is applicable	10	Select	0	
126	The solution shall provide configurable risk-, confidence- and policy-based controls for prioritizing alerts, incidents and automated actions, considering factors including detection confidence, asset criticality, user/entity risk, threat severity, business context and response-action type.	RFP Requirement is applicable	10	Select	0	

SIEM						
S.No.	Functional Specification	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
127	AI-generated findings, summaries, recommendations and investigation results shall, wherever technically supported, provide relevant contextual evidence and traceability to the underlying security events, alerts, entities, indicators, telemetry, analytics or threat-intelligence information used to derive such results.	RFP Requirement is applicable	10	Select	0	
128	The solution shall maintain comprehensive audit records of AI-assisted investigations, analyst activities and automated operations, including relevant recommendations, queries, approvals, executed actions, response outcomes and associated timestamps, subject to applicable retention requirements.	RFP Requirement is applicable	10	Select	0	
129	The proposed SIEM/NG-SIEM solution shall provide a unified incident-management and attack-story view that correlates security telemetry across endpoints, users, applications, network, cloud and other supported data sources, enabling analysts to investigate an incident from a single consolidated context and understand the sequence and relationships of related security activities.	RFP Requirement is applicable	10	Select	0	
130	The solution shall provide broad, pre-integrated and extensible integration and orchestration capabilities with the Bank's security ecosystem, including endpoint security, network security, firewalls, SOAR, IAM/PAM, email security, cloud security, vulnerability management, threat intelligence and other supported third-party security technologies.	RFP Requirement is applicable	10	Select	0	
131	The proposed cloud-delivered solution shall provide secure multi-tenant architecture with appropriate logical tenant isolation, encryption in transit and at rest, secure authentication, MFA, granular RBAC, audit logging and protection of Bank security data in accordance with the approved service architecture, security controls and SLA.	The proposed cloud-delivered solution shall provide secure tenant architecture with appropriate logical tenant isolation, encryption in transit and at rest, secure authentication, MFA, granular RBAC, audit logging and protection of Bank security data in accordance with the approved service architecture, security controls and SLA.	10	Select	0	
132	The bidder shall provide a complete bill of materials identifying all products, modules, capabilities, licenses, subscriptions, connectors, agents, APIs and third-party dependencies required to deliver the proposed SIEM, AI-driven analytics, investigation, threat hunting, automation, orchestration and response capabilities.	RFP Requirement is applicable	10	Select	0	
133	All mandatory capabilities proposed under the SIEM/NG-SIEM solution shall be generally available, production-ready and operational from Day 1 of production implementation. Any roadmap, beta, preview, technology-preview, optional or separately licensed capability shall be explicitly identified by the bidder and shall not be considered compliant with the mandatory requirement unless expressly accepted by the Bank.	RFP Requirement is applicable	10	Select	0	
134		An agentic security-operations platform where AI agents can plan, reason and execute SOC workflows, with controls such as analyst permissions and human approval for sensitive action	10	Select	0	
TOTAL MARKS			1530		0	

NOTE: Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or " Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal

UEBA					
S.No.	Functional Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
The OEM shall submit mandatory compliance with the Cloud Deployment requirements along with the Functional Specifications of the proposed solution.					
1	The UEBA must be able to monitor all the users in the organization. UEBA should not have separate data repository and should consume and operate on data avaialble within SIEM data repository. Use Case: Every single user can be source or a target of threat hence it's very important to cover all the users with UEBA solution.	10	Select	0	
2	The UEBA must create a heuristic baseline of user activity by analyzing behavior, so it must perform multidimensional baselining, enabling the modeling of a broad set of user behaviors. Baselines are used to detect anomalous behavior via machine learning and other statistical analysis techniques.	10	Select	0	
3	Investigate and respond to detected threats using a streamlined threat review workflow that provides visibility into anomalous activity and supporting evidence. Should increases the effectiveness of our security analysts by helping them focus on threats and malicious activities. with kill chain and geographical visualizations.	10	Select	0	
4	The proposed solution should use machine learning algorithms to analyze the data for activity deviating from normal behavior.	10	Select	0	
5	The proposed solution should have threat detection technique and models to distill anomalies down to a real handful threat. A single violation might not represent a legitimate threat in our environment. Over time, however, a series of violations should tell a story about a threat that must be investigated. Threat detection models should stitch together anomalies to provide an end-to-end story about a high-fidelity threat.	10	Select	0	
6	The proposed solution shall support dynamic log parsing and normalization upon ingestion. In cases where historical security telemetry must be re-parsed or remodeled under updated processing logic, the platform must provide high-speed, cloud-native ingestion pathways to re-ingest and re-process the historical log streams within the SIEM/platform repository without impacting active SOC performance, availability, or operational detection engines.	10	Select	0	
7	The proposed solution should have anomaly detection models to analyze the data in UBEA and create anomalies or violations based on a variety of factors.	10	Select	0	
8	The proposed solution should be able to create new anomaly detection rules/ models or clone existing models from the GUI.	10	Select	0	
9	The proposed solution should find deviations from typical behaviour or detection of interesting patterns like beaconing.	10	Select	0	
10	The proposed solution should detect threats using graph-based threats, which are computed based on groups of similar anomalies rather than anomalies grouped by user or device. Example graph-based threatsare public-facing website attack or fraudulent website activity. OR The proposed solution should detect threats using UEBA + AI Engine to detect anomalies and complex scenarios OR graph-based threats, which are computed based on groups of similar anomalies rather than anomalies grouped by user or device.	10	Select	0	
11	The proposed solution should detect threats like Lateral Movement and Data Ex-filtration. These should collect data about anomalies and users or devices to determine the likelihood of a threat.	10	Select	0	

UEBA					
S.No.	Functional Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
12	Solution should have parsers to capture logs, data , required infromation from SIEM as required for monitoring, analytics and reporting	10	Select	0	
13	UEBA threat detaction capabilites must be inline with Mitre Att&ck framework (Provide the documentation for the same)	10	Select	0	
14	UEBA and SIEM solution shoiuld be from same OEM. However if bidder is providing UEBA from different OEM then it should provide capability for single console from where both SIEM and UEBA can be monitered.	10	Select	0	
15	Solution UI/panel should be integrated in SIEM dashboard. Thus, which will help in monitor desired elements of users" behaviors, risks and trends	10	Select	0	
16	• File reputation	10	Select	0	
17	Application misuse by sequence of actions: User performs a sequence of actions which no other user is performing.	10	Select	0	
18	The solution should be capable to analyze the user and entity behavior, based on these behaviors analysis , the solution should generate comprehensive analysis	10	Select	0	
19	Solution should allow alerts for examination that shows the event in context of the user's baseline and other relevant entities in the enterprise.	10	Select	0	
20	The solution should be able to construct and fine tune hypothesis and define peer groups dynamically based on observed behavior, continuous evaluation, clustering, machine learning capabilities	10	Select	0	
21	The solution should be able to provide daily, weekly, monthly insights into risky users /entities based on risk score rating in the form of dashboards and reports.	10	Select	0	
22	Solution should provide most known use cases scush as - Compromised account - Data exfiltration - Privilage Account Misuse - Lateral movement etc.	10	Select	0	
23	The proposed solution is a fully managed, cloud-native SaaS platform that guarantees 99.9% uptime	10	Select	0	
24	The proposed solution shall feature a cloud-native SaaS delivery model that secures cloud workloads and hybrid SaaS environments through a single cloud console	10	Select	0	
25	Solution should cover the usage changes over time such as User activity deviates from normal over a short period of time or a gradual change over an extended period of time.	10	Select	0	
26	UEBA should perform identity resolution to find the real-time association between endpoints, IP addresses, host names, endpoint location, and users, and maintain these associations over time	10	Select	0	
27	Bidder has to supply on-inclusive license as per bank requirement from day 1 to meet the scope and specification mentioned in the RFP	10	Select	0	
28	The proposed solution should have self-learning algorithms (machine learning) to identify patterns of normal and malicious user and entity behaviour	10	Select	0	
TOTAL MARKS		280		0	

NOTE: Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or " Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the

Security Orchestration and Automation response (SOAR)					
S.No.	Functional Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
The OEM shall submit mandatory compliance with the Cloud Deployment requirements along with the Functional Specifications of the proposed solution.					
1	The proposed solution must have a orchestrator ability to direct and oversee all activities from beginning to end with Named user license (Count is mentioned in the RFP) with unlimited actions. Solution orchestrator must be able to ingest security data from any source and in any format. Example: Email based alerts SIEM based alerts	10	Select	0	
2	Proposed SOAR solution should have 70+ OOTB and should allow creation of 100s of playbooks. It should support OOTB integration with 100+ different OEM products. It should support more than 2500+ automated actions. It should have a bi-directional integration with SIEM solution. and can also be able to integrate with all industry leading SIEM solution. The OEM should additionally provide playbook creation, deletion, or custom integration services at no extra cost to the Bank in order to meet the rquirement stated in the RFP and Functional rquirement	10	Select	0	
3	To enable the virtual segregation of various data types, the proposed solution should support an unlimited number of virtual storage groups or indexes. Each index or virtual storage group should be designated for searching specific data, with a configurable retention period tailored to each index.	10	Select	0	
4	The proposed solution must provide a built-in visual automation editor. Proposed solution built-in visual automation editor must enable users to construct comprehensive and sophisticated playbooks to fully validate, investigate and resolve incident using drag and drop capabilities visually without needing the expert ability to code.	10	Select	0	
5	The proposed solution must provide an open and extensible interface for new integrations to connect the platform to any of the thousands of point products available in the security market today. Proposed solution must provide easy transition in and out of other security technologies without negatively impacting automated playbooks. Proposed solution must provide users with the framework and open control of integrating with other technologies without relying on the solution provider for development work.	10	Select	0	
6	The proposed solution shall support dynamic log parsing and normalization upon ingestion. In cases where historical security telemetry must be re-parsed or remodeled under updated processing logic, the platform must provide high-speed, cloud-native ingestion pathways (via HTTP log collectors, API-based ingestion, or other proposed cloud-native mechanism) to re-ingest and re-process the historical log streams within the SIEM/platform repository without impacting active SOC performance, availability, or operational detection engines	10	Select	0	
7	The proposed solution must have documented REST API access that allows full control over the platform. It must have ability to label the nature of the event. It must also have ability to store attachment as part of the user manual workflow or as part of the automated playbook. It must be able to extract and store attchments from ingested emails. It must have the ability to mark artifacts as evidence. It must be able to provide an indicator view to quickly pivot investigation of an indicator to past incident occurences. It must allow case or task assignment in relation to a ticket or an incident to other team members or group.	10	Select	0	
8	The proposed solution must provide fine grained role-based access into actions and assets, so users can be granted with investigative actions and not containment actions. Proposed solution must have an activity log of actions taken (automated and manual), results returned by actions, chat and comment history in each event. Proposed solution must provide central management of incidents and administrative functions from a single web based user interface.	10	Select	0	

Security Orchestration and Automation response (SOAR)					
S.No.	Functional Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
9	Proposed solution should offers extensive and flexible case management functionality. Case attributes can be customized, and artifacts can be attached to the case, such as a phishing message, IOC, file, etc. Case management workflows can easily be automated by using the Visual Playbook Editor. In addition, it should allows workbooks to be attached to cases representing "people processes" or processes an analyst would take in their investigation. It should also allows real - time collaboration between security analysts.	10	Select	0	
10	Solution should provide Role Based Access (RBAC) to differentiate between analysts and administrators for restricting access to investigations, Jobs, Scripts, playbooks and admin tasks.	10	Select	0	
11	Solution should be able to integrate with security devices like AD, Firewall, IPS, endpoint Security solution, APT solution, WAF, Proxy, DLP etc from day one	10	Select	0	
12	Solution must have an authenticated API capable of executing the same functions as are available via the GUI	10	Select	0	
13	Solution should have its own SDK (software development kit) for integration purpose	10	Select	0	
14	Solution should support standard languages like Python to create and customize scripts for custom integrations	10	Select	0	
15	Solution should support SAML 2.0 or 2 Factor Authentication	10	Select	0	
16	Solution Should allow creation of Manual Tasks, Automated Tasks, scheduled tasks and Conditional Tasks in Playbooks	10	Select	0	
17	Solution should record all manual and automated entries during execution with timestamp for a case for audit purpose	10	Select	0	
18	Solution should maintain SLA for incident	10	Select	0	
19	Solution should support sending notifications to other users on incident basis	10	Select	0	
20	Solution should integrate with Incident management tools and IT ticketing system (third party)	10	Select	0	
21	The solution must have a provision to remove duplicate incidents and DeDupe all similar alerts.	10	Select	0	
22	The proposed solution is a fully managed, cloud-native SaaS platform that guarantees 99.9% uptime	10	Select	0	
23	The proposed solution shall feature a cloud-native SaaS delivery model that secures cloud workloads and hybrid SaaS environments through a single cloud console	10	Select	0	
24	Solution should support mock data/Incidents to debug, test, or troubleshoot playbook during creation.	10	Select	0	
25	The solution should have capability to assign incidents/ tickets based on type of incident, asset owner, concerned department, work-load on analyst etc.	10	Select	0	
26	The solution should shall allow to create custom playbooks as and when required.The playbooks should support: a. Time based actions b. Escalation actions c. Automated Tasks in Playbooks d. Record all manual and automated entries during execution of a playbook e. Complete playbook to be run automatically or manually and list out any exceptions.	10	Select	0	
27	The solution must be able to provide incident response playbooks that consist of phases and tasks that guides the user on how to adequately respond to the incident, integrating people, processes, and technology.	10	Select	0	
28	The solution must support incident enrichment using IOCs and Indicators of Attack (IOA) received from Threat Intel feeds and unstructured threat intelligence received over email, file etc.	10	Select	0	
29	The solution should be able to send notification to end users such as (but not limited to) via Email/SMS during the investigation.	10	Select	0	
30	The solution should support SSO integration with on- premises Active Directory, LDAP, etc.	10	Select	0	
31	The alert and incident management interfaces should be customizable to allow flexible information display, including displaying information from the alert itself plus additional information returned by investigative playbooks.	10	Select	0	
32	Tickets escalation should be based on: Priority, Risk, Impact or Age.	10	Select	0	

Security Orchestration and Automation response (SOAR)					
S.No.	Functional Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
33	When an alert or incident closed manually, the solution should mandate the closure reason to be provided for audit and select the category for the closure, such as - duplicate, externally resolved, not a threat etc.	10	Select	0	
34	The solution should provide a no-code/low-code, drag- and-drop-based response design for the creation of simple or advanced playbooks.	10	Select	0	
35	Bidder has to supply on-inclusive license as per bank requirement from day 1 to meet the scope and specification mentioned in the RFP	10	Select	0	
36	The proposed solution must provide an open and extensible interface for new integrations to connect the platform to any of the thousands of point products available in the security market today and it must provide users with the framework and open control of integrating with other technologies without relying on the solution provider for development work.	10	Select	0	
37	The solution must not block, drop, or place grace period when system exceeds license count.	10	Select	0	
38	The playbooks should support:				
38.1	- nested playbooks to deploy multiple automations as part of a single use case	10	Select	0	
38.2	- conditional decision trees	10	Select	0	
38.3	- user inputs or inputs from various stakeholders in the use case/reviews	10	Select	0	
38.4	- status-based decisions	10	Select	0	
38.5	- escalation actions	10	Select	0	
39	Integration packs should include pre-built use cases consisting of playbooks, automation actions, scripts that can be customised for Bank's SOC. The solution should have an integration store that is continuously updated with both OEM and bidder provided integration.	10	Select	0	
40	The solution must have out-of-the-box use cases ecosystem including but not limited to the following technologies:	-	-	-	
40.1	- Forensics tools (e.g. FTK, EnCase, Autopsy…)	10	Select	0	
40.2	- IT (e.g. AD, SAM…)	10	Select	0	
40.3	- Communications tools (e.g. email, Slack, HipChat…)	10	Select	0	
40.4	- SIEM tool	10	Select	0	
40.5	- Endpoint Security	10	Select	0	
40.6	- Network Security	10	Select	0	
40.7	- Active Directory	10	Select	0	
40.8	- Threat Intelligence	10	Select	0	
40.9	- Dynamic malware analysis	10	Select	0	
41	The solution should offer the ease of creating custom playbooks which needs to be flexible and multi-conditional.	10	Select	0	
42	The proposed solution shall provide AI-assisted security operations capabilities to support alert analysis, incident investigation, threat hunting, incident summarization, security-data correlation and response recommendations.	10	Select	0	
43	The solution shall provide AI-assisted natural-language investigation and query capabilities to enable SOC analysts to investigate security events, understand incident context and identify relevant security findings.	10	Select	0	
44	The solution shall support AI-assisted alert correlation, prioritization and investigation across available endpoint, network, identity, application and threat-intelligence data.	10	Select	0	
45	The solution shall support security orchestration and automated response through configurable playbooks/workflows, enabling automated enrichment, investigation, containment and response actions across supported security technologies.	10	Select	0	
46	The solution shall support analyst-controlled and policy-based automated response, including configurable approval mechanisms for actions that require human validation before execution.	10	Select	0	

Security Orchestration and Automation response (SOAR)					
S.No.	Functional Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
47	The solution shall provide RBAC, authentication and least-privilege controls for security operations, automation, playbooks, integrations and response activities.	10	Select	0	
48	The solution shall maintain audit trails for security automation and response activities, including triggering events, executed actions, relevant integrations, approvals and execution results, as applicable.	10	Select	0	
49	The solution shall support integration with enterprise security technologies including endpoint security, network security, firewalls, threat intelligence, identity/security platforms, vulnerability-management solutions, ITSM and other supported security products through native integrations, APIs or connectors.	10	Select	0	
50	The solution shall provide monitoring and management of automation workflows and integrations, including visibility into connectivity, authentication, execution and integration failures and appropriate troubleshooting information.	10	Select	0	
51	The solution shall support playbook/workflow development, testing, modification and controlled deployment, enabling authorized security administrators to manage security automation throughout its operational lifecycle.	10	Select	0	
52	The solution shall provide AI-assisted threat hunting and investigation capabilities, including natural-language or query-assisted investigation, correlation of relevant security telemetry and contextual enrichment of identified threats.	10	Select	0	
53	The solution shall provide threat-intelligence enrichment and contextual analysis as part of security investigation, threat hunting and incident-response workflows.	10	Select	0	
54	The solution shall support automated enrichment and response actions using configurable workflows and integrations, subject to applicable security policies, authorization and access controls.	10	Select	0	
55	The solution shall provide configurable automation safeguards and execution controls, including role-based restrictions, action authorization and controls for sensitive or high-impact response activities.	10	Select	0	
56	All mandatory security operations, AI-assisted, orchestration and automation capabilities proposed as part of the solution shall be generally available and operational from Day 1 of production implementation. Any separately licensed, optional or third-party-dependent capability shall be clearly identified in the bidder's response.	10	Select	0	
TOTAL MARKS		680		0	

NOTE:	Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or " Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product

XDR						
S.No	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
	Extended Detection and Response					
The OEM shall submit mandatory compliance with the Cloud Deployment requirements						
1	XDR platform should be able to integrate with third party security vendors like Firewall, by ingesting logs for better correlation, in syslog/CEF/LEEF format	RFP Requirement is applicable	10	Select	0	
2	The proposed XDR solution must employ advanced machine learning algorithms and behavioural analysis techniques to detect and respond to threats in real-time.	RFP Requirement is applicable	10	Select	0	
3	The proposed XDR solution should offer centralized visibility and control over all managed endpoints through a unified management console. This console should enable administrators to monitor, manage, and respond to security incidents across the entire network from a single interface. Features should include real-time monitoring, incident response capabilities, comprehensive reporting, and customizable dashboards. Documentation of the unified management capabilities should be provided.	RFP Requirement is applicable	10	Select	0	
4	The proposed XDR solution should implement a layered defence strategy to filter out threats using advanced tactics and techniques. It should have but following prevention capabilities:	Clause Stands Deleted				
4.1	The proposed solution shall support dynamic log parsing and normalization upon ingestion. In cases where historical security telemetry must be re-parsed or remodeled under updated processing logic, the platform must provide high-speed, cloud-native ingestion pathways (via HTTP log collectors, API-based ingestion, or other proposed cloud-native mechanism) to re-ingest and re-process the historical log streams within the SIEM/platform repository without impacting active SOC performance, availability, or operational detection engines	RFP Requirement is applicable	10	Select	0	
4.2	• Ransomware protection	RFP Requirement is applicable	10	Select	0	
4.3	• Machine learning - pre-execution and runtime / Signature-less	RFP Requirement is applicable	10	Select	0	
4.4	• Browser exploit protection	RFP Requirement is applicable	10	Select	0	
4.5	• Behavior monitoring	RFP Requirement is applicable	10	Select	0	
4.6	• Polymorphic attack prevention	RFP Requirement is applicable	10	Select	0	
4.7	• Script protection	RFP Requirement is applicable	10	Select	0	
4.8	• Anti-exploit	RFP Requirement is applicable	10	Select	0	
4.9	• C&C communication prevention	RFP Requirement is applicable	10	Select	0	
4.10	• File less malware prevention	RFP Requirement is applicable	10	Select	0	
4.11	• File reputation	RFP Requirement is applicable	10	Select	0	
4.12	• Sandboxing of files	RFP Requirement is applicable	10	Select	0	
4.13	• The goal is to minimize the attack surface by continuously monitoring, updating, and provide compensatory controls for vulnerabilities and exploits in the endpoints	RFP Requirement is applicable	10	Select	0	
5	The proposed XDR solution should have comprehensive threat remediation capabilities, including cleaning infected files, performing rollback of malicious changes, and showcase the changes	RFP Requirement is applicable	10	Select	0	
6	The proposed XDR solution should ensure a good user experience by minimizing impact on endpoint performance. This can be achieved through optimized detection techniques, efficient resource management, and low CPU usage during endpoint scanning.	RFP Requirement is applicable	10	Select	0	
7	The proposed XDR solution must ensure off-premises compliance and protection, allowing employees to work securely from remote locations. It should extend the same level of endpoint security to remote workers, ensuring all devices remain protected and compliant with corporate security policies.	RFP Requirement is applicable	10	Select	0	

XDR						
S.No	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
8	The Solution should support agent version control, to ensure "n", "n-1", "n-2" agent version can be deployed as per the process laid by PSB	RFP Requirement is applicable	10	Select	0	
9	The proposed solution is a fully managed, cloud-native SaaS platform that guarantees 99.9% uptime"	RFP Requirement is applicable	10	Select	0	
10	The proposed solution shall feature a cloud-native SaaS delivery model that secures cloud workloads and hybrid SaaS environments through a single cloud console	RFP Requirement is applicable	10	Select	0	
11	The proposed XDR solution must include robust ransomware protection mechanisms, including real-time monitoring and protection features that detect and prevent ransomware activities.	RFP Requirement is applicable	10	Select	0	
12	The proposed solution must provide protection against malicious AI application tampering on the endpoints	RFP Requirement is applicable	10	Select	0	
13	The proposed solution must offer anti-tamper proofing, so that users/threat actors cannot make modifications in the agent features or deletion of agent	RFP Requirement is applicable	10	Select	0	
14	The proposed XDR solution must provide comprehensive alert management capabilities, including generating a list of alerts triggered by detection logic, allowing administrators to investigate and respond to each alert, and enabling changing the status of alerts based on the stage of the investigation.	RFP Requirement is applicable	10	Select	0	
15	The proposed XDR solution must provide comprehensive activity data management and search capabilities, including receiving activity data in the form of telemetry, and metadata; feature for automatic query runs and email notifications; threat matching features using Boolean Logic and other criteria; and options to export, import, delete, and share saved search queries.	RFP Requirement is applicable	10	Select	0	
16	The proposed XDR solution must provide the capability to perform a comprehensive sweep and assessment of the current state of devices, including scanning disk files, in-memory processes, and registry.	RFP Requirement is applicable	10	Select	0	
17	The solution must collect, organize, and provide an up-to-date information resource for active Threat Campaigns including information such as, Infection Chain, MITRE ATT&CK mapping, Intelligence Data, and Impact Scope. It should have a feature to display ongoing attacks if any indicators signal the same, enabling timely prevention, investigation, and mitigation actions against targeted attack campaigns	RFP Requirement is applicable	10	Select	0	
18	the proposed solution should allow to create & save custom queries so analysts can find data quickly and perform faster threat hunting	RFP Requirement is applicable	10	Select	0	
19	The solution should display a list of suspicious objects based on third-party intelligence, sandbox, and user-defined keywords. It should provide a feature to add suspicious objects manually on the parameters/Indicators of Compromise (IOCs).	RFP Requirement is applicable	10	Select	0	
20	The solution should be able to create multi-stage detailed kill-chain for performing root cause analysis of an incident. The kill chain must also provide the reputation of the files from the global threat intelligence.	RFP Requirement is applicable	10	Select	0	
21	The solution should provide advanced response capabilities, including isolating devices, blocking processes, collecting evidence, dumping process memory, initiating remote shell sessions, running OS queries, restoring connections, running remote custom scripts or running YARA rules, scanning for malware, adding to block lists, and removing from block lists.	RFP Requirement is applicable	10	Select	0	
22	The solution should offer options to leverage anti-malware and anti-spyware components stored locally on agents, or signatures stored in-the-vendor cloud	RFP Requirement is applicable	10	Select	0	
23	Machine learning must have Pre-execution intelligence of extracting file features and run-time analysis of file/process behavior to identify threats.	RFP Requirement is applicable	10	Select	0	

XDR						
S.No	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
24	The solution must have behavior monitoring module to constantly monitor endpoints for unusual modifications to the operating systems or on installed software's to provide additional threat protection from programs that exhibit malicious behavior.	RFP Requirement is applicable	10	Select	0	
25	The solution must provide a protection mechanism against ransomware in the event of a machine becoming compromised and should have feature with documents to be protected from unauthorized encryption or modification.	RFP Requirement is applicable	10	Select	0	
26	The solution must have Anti-exploit module to terminate the program exhibiting abnormal behavior associated with exploit attacks. Solution must be able to detect multiple exploit techniques like memory corruption, logic flaw, malicious code injection/execution.	RFP Requirement is applicable	10	Select	0	
27	The solution must be able to identify communication over HTTP/HTTPS protocols and commonly used HTTP ports, it must be able to detect/prevent communications to Global C&C's and Allow administrators to create user defined list also.	RFP Requirement is applicable	10	Select	0	
28	The solution must support host-based firewall with stateful inspection, option to create rules on the basis of Source/Destination/Port/Protocol/Application to provide stateful inspection and high performance network virus scanning	RFP Requirement is applicable	10	Select	0	
29	The solution Device Control capability must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The solution Device Control capability must support Network Devices, USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, time based device control capabilities allowing admin to define the policy specifically for the endpoint operating systems (Windows 10, 11 or higher).	RFP Requirement is applicable	10	Select	0	
30	The Devices that are able to be restricted must include but not limited to the following:	Clause Stands Deleted				
30.1	USB Storage Drives (Also able to disable autorun)	RFP Requirement is applicable	10	Select	0	
30.2	CD-ROM	RFP Requirement is applicable	10	Select	0	
30.3	Floppy Disk	RFP Requirement is applicable	10	Select	0	
30.4	Network Drives	RFP Requirement is applicable	10	Select	0	
31	The solution must have damage cleanup services to provide automated cleanup of the changes made by the malware including network and file-based malicious applications, and virus and worm remnants (Trojans, registry entries, and viral files).	RFP Requirement is applicable	10	Select	0	
32	Should include predefined detection models which combine multiple rules, and filters using techniques such as machine learning and data stacking. Should be regularly updated to improve threat detection capabilities and reduce false positive alerts and it should have the ability to enable or disable detection models and add/configure detection model exceptions based on the organization requirements.	RFP Requirement is applicable	10	Select	0	
33	Should allow the creation of custom detection models and custom event filters that define the events the model uses to trigger alerts.	RFP Requirement is applicable	10	Select	0	
34	The solution should be able to analyze and determine if certain indicators signal an ongoing attack, enabling SOC team to take timely prevention, investigation, and mitigation actions against targeted attacks.; by analying the logs of endpoint protection solution	RFP Requirement is applicable	10	Select	0	
35	The console should provide different search methods, filters, and an easy-to-use Kibana-like query language or any other query language to identify, categorize, and retrieve search results and	RFP Requirement is applicable	10	Select	0	
36	The proposed solutio should provide an functionality to administrator to add or remove indicators of compromise to block list including but not limited to File hash, URL, IP address, and Domains.	RFP Requirement is applicable	10	Select	0	
37	The proposed solution must provide the below response capabilities:	Clause Stands Deleted				

XDR						
S.No	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
37.1	Remotely connect to an endpoint and dump process memory.	RFP Requirement is applicable	10	Select	0	
37.2	Remote isolation of an endpoint but still maintain communication with the management server to continue with investigation.	RFP Requirement is applicable	10	Select	0	
37.3	Ability to remotely connect and execute custom PowerShell or Bash scripts.	RFP Requirement is applicable	10	Select	0	
37.4	Remote shell session capability and be able to execute remote commands	RFP Requirement is applicable	10	Select	0	
37.5	Submit selected file or object for automated analysis in a sandbox, a secure virtual environment.	RFP Requirement is applicable	10	Select	0	
37.6	Ability to view and terminate active processes on a specific endpoint or multiple endpoints.	RFP Requirement is applicable	10	Select	0	
38	The solution should allow a SOC analyst to manually add IoCs such as File Hashes, IP Addresses, Domains, and URL's as part of the custom intelligence. It should also allow a SOC analyst to build custom intelligence by subscribing to third-party threat intelligence feeds.	RFP Requirement is applicable	10	Select	0	
39	To optimize the bandwidth solution should support update agent/edge relay where one or more endpoint can download component updates and push it to other endpoints in PSB environment	RFP Requirement is applicable	10	Select	0	
40	Solution should offer customizable level of degree of vigilance and strictness applied when detecting and responding to potential threats via the detection & response sensor	RFP Requirement is applicable	10	Select	0	
41	The proposed solution should enable administrators to manage and restrict access. This feature should facilitate control over which endpoints can access or execute designated files/folders, thereby enhancing overall security and ensuring compliance with organizational policies.	RFP Requirement is applicable	10	Select	0	
42	The proposed solution should provide recommended actions to address and mitigate threats detected on endpoints. These remediation suggestions should be informed by forensic data collected from endpoints and detailed analysis performed by the solution to enhance threat response and resolution.	RFP Requirement is applicable	10	Select	0	
43	The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature or through seamless integration with a third-party sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data	The proposed solution must include functionality to perform sandbox analysis of suspicious files, provided as a native capability	10	Select	0	
44	The proposed solution should provide real-time anti-exploit capabilities to protect customer's assets from exploit attacks including but not limited to memory corruption, logic flaw, malicious code injection/execution, DLL Hijacking, etc.	RFP Requirement is applicable	10	Select	0	
45	The proposed solution must allow administrators to manage and control temporary exceptions for trusted devices if needed	RFP Requirement is applicable	10	Select	0	
46	The solution should be capable to integrate with AD/AzureAD/EntraID for identity threat detection & response; and take response actions on the users as well	RFP Requirement is applicable	10	Select	0	
47	The centralized management console of the proposed XDR must integrate with Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) systems. This integration should enable streamlined data sharing, improved incident response, and enhanced overall security management. The solution should offer a customizable dashboard that allows different administrators to personalize their view by selecting specific summaries and metrics they wish to see.	RFP Requirement is applicable	10	Select	0	
48	The proposed XDR solution shall provide capabilities aligned with industry-recognized threat frameworks, including MITRE ATT&CK, and shall provide relevant documentation demonstrating threat detection and mapping capabilities.	RFP Requirement is applicable	10	Select	0	

XDR						
S.No	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
49	The proposed XDR solution should provide AI-assisted investigation capabilities to support analysts with threat analysis, contextual insights, investigation guidance, and response recommendations.	RFP Requirement is applicable	10	Select	0	
50	The proposed XDR solution in its entirety (XDR software, management console, and related services) must comply with industry standards such as ISO/IEC 27001, or relevant regional regulations. It should be completely based in India, with MeitY empanelled Cloud data centres. The vendor must provide compliance certificates and documentation. Data should not be transferring or storing any data outside India.	RFP Requirement is applicable	10	Select	0	
51	Bidders must propose a solution which is easy-to-manage, clientless platform that gets deployed quickly and involves minimal or no dependency on customization and management of operating environment.	RFP Requirement is applicable	10	Select	0	
52	The proposed solution shall support required Bank-side components at the Bank's Data Center (DC) and Disaster Recovery (DR) sites, as applicable, to facilitate secure connectivity between the Bank's intranet (endpoints, servers, and network) and the cloud-hosted solution. If any required component is not available as part of the proposed solution, the Bidder shall provide the necessary third-party hardware, software, proxy servers, enterprise licenses, and associated support at no additional cost to the Bank.	RFP Requirement is applicable	10	Select	0	
53	Easy-to-manage, clientless platform that deploys quickly and involves minimal or no dependency on customization and management.	RFP Requirement is applicable	10	Select	0	
54	Perimeter Analytics should have well defined work flow for response mechanism along with integration from F/w, XDR, SOAR and SIEM	RFP Requirement is applicable	10	Select	0	
55	The solution should provide a RESTful API and should be integrated with security orchestration (SOAR) to implement response actions.	RFP Requirement is applicable	10	Select	0	
56	Support SNMP/syslog etc. for integration with all leading SIEM/SOC solutions. The Solution components should also be providing access over REST API's with detailed OEM documentation. The Solution must only be accessible via web UI and shall not require any plugins or thick client requirements for Admins and Analysts access.	RFP Requirement is applicable	10	Select	0	
57	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	RFP Requirement is applicable	10	Select	0	
58	Web based GUI and a unified security dashboard displaying the real time consolidated data in graphical/textual format and all alerts received from and detected by all the traffic. The solution should have the ability to view and identify the infected systems and drill down into infection details at centralized location..	RFP Requirement is applicable	10	Select	0	
59	Central management solution must have capability to enable remote management and configurations	RFP Requirement is applicable	10	Select	0	
59.1	Solution should be able to integrate with 3rd party solution like:	Clause Stands Deleted				
59.2	Breach Assessment and Simulation	RFP Requirement is applicable	10	Select	0	
59.3	Firewall and Network	RFP Requirement is applicable	10	Select	0	
59.4	ITSM	RFP Requirement is applicable	10	Select	0	
59.5	SIEM	RFP Requirement is applicable	10	Select	0	
59.6	SOAR	RFP Requirement is applicable	10	Select	0	
59.7	Threat Intel	RFP Requirement is applicable	10	Select	0	
59.8	UEM, UEBA and ITDR	RFP Requirement is applicable	10	Select	0	
59.9	Vulnerability Management	RFP Requirement is applicable	10	Select	0	

XDR						
S.No	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
59.10	Threat Intelligence	RFP Requirement is applicable	10	Select	0	
59.11	Any other security solution	RFP Requirement is applicable	10	Select	0	
60	Proposed Solution should offer granular role based access control policy for accessing the console	RFP Requirement is applicable	10	Select	0	
61	Solution should have the capabilities to create and run security playbooks for automation and better MTTD/MTTR on the basis of criticality of threat/server	RFP Requirement is applicable	10	Select	0	
62	Solution should provide out of the box report both on the console as well as over email in CSV, PDF or RTF format	RFP Requirement is applicable	10	Select	0	
63	The proposed solution should have centralized management	RFP Requirement is applicable	10	Select	0	
22	The solution will offer a 360-degree identity view for all users and systems, providing a comprehensive understanding of their attributes, access, and historical behavior.	RFP Requirement is applicable	10	Select	0	
23	Easy-to-manage, clientless platform that deploys quickly and involves minimal or no dependency on customization and management.	RFP Requirement is applicable	10	Select	0	
24	Perimeter Analytics should have well defined work flow for response mechanism along with integration from F/w, XDR, SOAR and SIEM	RFP Requirement is applicable	10	Select	0	
25	The solution should provide a RESTful API and should be integrated with security orchestration (SOAR) to implement response actions.	RFP Requirement is applicable	10	Select	0	
26	Support SNMP/syslog etc. for integration with all leading SIEM/SOC solutions. The Solution components should also be providing access over REST API's with detailed OEM documentation. The Solution must only be accessible via web UI and shall not require any plugins or thick client requirements for Admins and Analysts access.	RFP Requirement is applicable	10	Select	0	
27	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	RFP Requirement is applicable	10	Select	0	
28	Web based GUI and a unified security dashboard displaying the real time consolidated data in graphical/textual format and all alerts received from and detected by all the traffic. The solution should have the ability to view and identify the infected systems and drill down into infection details at centralized location..	RFP Requirement is applicable	10	Select	0	
29	Central management solution must have capability to enable remote management and configurations	RFP Requirement is applicable	10	Select	0	
30	Solution should be able to integrate with 3rd party solution like:	Clause Stands Deleted				
30.1	Breach Assessment and Simulation	RFP Requirement is applicable	10	Select	0	
30.2	Firewall and Network	RFP Requirement is applicable	10	Select	0	
30.3	ITSM	RFP Requirement is applicable	10	Select	0	
30.4	SIEM	RFP Requirement is applicable	10	Select	0	
30.5	SOAR	RFP Requirement is applicable	10	Select	0	
30.6	Threat Intel	RFP Requirement is applicable	10	Select	0	
30.7	UEM, UEBA and ITDR	RFP Requirement is applicable	10	Select	0	
30.8	Vulnerability Management	RFP Requirement is applicable	10	Select	0	
30.9	Threat Intelligence	RFP Requirement is applicable	10	Select	0	
30.10	Any other security solution	RFP Requirement is applicable	10	Select	0	
31	Proposed Solution should offer granular role based access control policy for accessing the console	RFP Requirement is applicable	10	Select	0	
32	Solution should have the capabilities to create and run security playbooks for automation and better MTTD/MTTR on the basis of criticality of threat/server	RFP Requirement is applicable	10	Select	0	

XDR						
S.No	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
33	Solution should provide out of the box report both on the console as well as over email in CSV, PDF or RTF format	RFP Requirement is applicable	10	Select	0	
34	The proposed solution should have centralized management	RFP Requirement is applicable	10	Select	0	
35	The solution will offer a 360-degree identity view for all users and systems, providing a comprehensive understanding of their attributes, access, and historical behavior.	RFP Requirement is applicable	10	Select	0	
36		The proposed solution shall provide Network Behaviour Anomaly Detection using available network telemetry and shall continuously establish and update traffic baselines to identify anomalies relating to traffic volume, traffic directionality, protocol usage, application usage, previously unseen applications, abnormal communication patterns and unusual host, endpoint or user behaviour, wherever user attribution is available.	10	Select	0	
37		The proposed solution shall detect network-based threats including, but not limited to, Command and Control communication, malware communication, lateral movement, network reconnaissance, data exfiltration, suspicious remote access, anomalous network behaviour and communication with known malicious IP addresses, domains and URLs.	10	Select	0	
38		The proposed solution shall support historical investigation of network activities using available network flow, metadata, session, packet-derived and other network telemetry and shall allow analysts to pivot from a network event to associated endpoint, identity, threat intelligence and other security events.	10	Select	0	
39		The proposed solution shall provide network threat response capabilities through native functionality and/or integration with applicable security controls, including blocking of malicious IP addresses, domains and URLs, network communication blocking, endpoint isolation, firewall/security-control policy updates and initiation of automated response workflows, wherever supported by the proposed architecture.	10	Select	0	
40		The proposed solution shall support integration with the Bank's SIEM and SOAR platforms through standard interfaces, including RESTful APIs, Syslog and other industry-standard mechanisms, for exchange of network alerts, incidents, Indicators of Compromise, telemetry and response actions.	10	Select	0	
41		The proposed solution shall provide root cause analysis and identify the probable attack sequence, affected assets, associated Indicators of Compromise and applicable MITRE ATT&CK tactics, techniques and procedures based on available XDR and network telemetry.	10	Select	0	
42		The proposed solution shall support detection and correlation of network activity with threat intelligence, including malicious IP addresses, domains, URLs, file hashes and other relevant indicators, and shall allow analysts to use such intelligence for threat hunting and detection.	10	Select	0	
43		The proposed solution shall provide configurable risk/severity prioritization for network detections based on factors including severity, confidence, asset criticality, threat intelligence and observed behaviour.	10	Select	0	

XDR						
S.No	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
44		The proposed solution shall support automated and analyst-approved response actions based on configurable policies, threat severity and confidence. The solution shall maintain an audit trail of automated and manual response actions.	10	Select	0	
45		The proposed solution shall support identification of infected or potentially compromised systems from network detections and shall provide drill-down capability into associated network activities, affected assets, users and related security events.	10	Select	0	
46		The proposed solution shall provide APIs and standard integration mechanisms for integration with Firewall, SIEM, SOAR, Threat Intelligence Platform, Identity and Access Management, User and Entity Behaviour Analytics, Vulnerability Management, IT Service Management and other security solutions.	10	Select	0	
47		The proposed solution shall support granular role-based access control for XDR and NDR functionality and shall maintain audit logs for administrative activities, investigations, configuration changes and response actions.	10	Select	0	
48		The proposed solution to use network metadata, flow information, session information and/or packet-derived telemetry for network detection, investigation and threat hunting.	10	Select	0	
49		Proposed solution must provide full Detection, Network Visibility, Investigation & Forensic capability / Back in Time investigation, through high speed lossless packet capture & analysis functions for a network traffic capture for 10 Gbps.	10	Select	0	
50		The solution shall support Network Behaviour Anomaly Detection using available network telemetry and shall provide Layer 3, Layer 4 and Layer 7 visibility, including relevant network, protocol, application, session and communication information, as supported by the proposed architecture. The system shall continuously learn and update the traffic behaviour baseline and shall detect deviations from the established baseline with respect to traffic volume, traffic directionality, protocol usage, application usage, previously unseen applications, abnormal communication patterns and anomalous behaviour of specific hosts, endpoints or users, wherever such information is available.	10	Select	0	
TOTAL MARKS			1160		0	

Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or " Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product

NDR					
S.No	Required Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
	Network Detection and Response	ALL NDR corresponding capabilities should be demonstrated through the proposed XDR platform, refer revised XDR specification			
TOTAL MARKS		**0**		**0**	

Application Security testing tool					
S.No	Required Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
1	The solution must be able to perform source code scanning and pinpoint the root cause of software security vulnerabilities	10	Select	0	
2	The solution must be able to integrate with SDLC to perform Code Review checks at the time of development	10	Select	0	
3	The solution must be able to analyse a wide array of programming languages including Java, .Net, C/C++, Objective-C, Android, PHP, COBOL, Ruby, Swift, HTML 5, Scala, APEX, TypeScript, Go, Kotlin and ABAP etc but not limited to these alone	10	Select	0	
4	The solution must support a variety of operating systems: Windows, Linux, MacOS, AIX, Solaris	10	Select	0	
5	The solution must be able to operate in both distributed (i.e., without requiring connection to a server) and centralized modes	10	Select	0	
6	The solution must offer the flexibility to begin, continue and end a scan locally without requiring connection to a centralized server	10	Select	0	
7	The solution must have regular (at least quarterly) updates to its vulnerability/rule's knowledgebase	10	Select	0	
8	The solution must provide the capability to create custom checks via a wizard	10	Select	0	
9	Custom checks created must be in an easily understood format, e.g., XML	10	Select	0	
10	Existing custom checks must continue to work without any additional effort when there is a version upgrade	10	Select	0	
11	The solution must support a variety of static analysis techniques including multi-tier multi-language data flow analysis, global control flow analysis, programmatic structural analysis, semantic analysis	10	Select	0	
12	The solution must support automated invocation of source code scans and vulnerability data report generation through integration with the application build process.	10	Select	0	
13	The solution shall provide a default prioritization of vulnerabilities according to severity and risk but offers the flexibility to change the prioritization easily according to organizational needs.	10	Select	0	
14	The solution must report vulnerabilities that have been fixed, newly introduced, or continue to exist across multiple scans.	10	Select	0	
15	Any issue marked as a false positive or suppressed automatically retains the status in the next scan	10	Select	0	
16	The solution shall maintain knowledge of vulnerabilities within code bases. Vulnerabilities found should not be tagged to LOC (line of code) position within the source codes, to avoid the loss of history should there be insertion of new codes	10	Select	0	
17	The solution allows the user to "drill down" to and "trace through" the suspect source code and show the root cause and supporting evidence of vulnerability in textual and pictorial formats.	10	Select	0	
18	The solution must provide vulnerability explanation and fix recommendations to the developer during the vulnerability remediation process, including line-of-code details and descriptions on how to remediate each vulnerability, and in the correct programming language.	10	Select	0	
19	The solution supports collaborative auditing where multiple auditors can work on the same scan result and audit the scan at the same time through a common user interface.	10	Select	0	
20	The solution has the capability to generate out-of-the-box and custom reports such as high-level executive analysis summaries and low-level (detailed) technical reports.	10	Select	0	
21	The solution must support separation of the code translation and analysis phases, which may be run on different machines. This allows the offloading of complex CPU and IO intensive codebase parsing off the developers' workstation, application servers, or version management servers and onto dedicated analysis appliances or servers.	10	Select	0	
22	The solution integrates with a defect-tracking system (e.g., HP ALM, QC Enterprise, Microsoft TFS, JIRA, Bugzilla, VSTS) for easy creation of defects for vulnerabilities found from within the solution itself.	10	Select	0	
23	The solution shall integrate into a web management console, to be correlated with security vulnerabilities found from dynamic and interactive testing for a holistic view of the security status of applications and projects within an enterprise.	10	Select	0	

Application Security testing tool					
S.No	Required Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
24	Solution should support Machine learning and Analysis based on the archived results	10	Select	0	
25	Solution should provide Immediate identification of the vulnerability in the Eclipse and VS IDEs while developer is typing the code	10	Select	0	
26	The solution should have the ability to identify the root cause of multiple other vulnerabilities and pinpoint the exact line in the source code to remediate	10	Select	0	
27	The solution must have Security Assistant feature to aid developers to find vulns while typing the code	10	Select	0	
28	The solution should be able to provide Just in Time learning on secure code enablement to get trainined on Vulnerabilities	10	Select	0	
29	The solution should be able to perform scan offline (translate in one machine and scan in another)	10	Select	0	
30	Solution should support Out of the Box integration capabilities with dev-ops supporting multiple Build environments - Jenkins, Maven, ANT, XCode Build, MS Build, Gradle etc.	10	Select	0	
31	The solution must be capable to address open-source risk	10	Select	0	
32	The solution should be able to support Composition Analysis: Identify the opens source components used in the application Vulnerabilities & outdated version Licensing risk associated with the components	10	Select	0	
33	The solution must come with a Dashboard to show enterprise-wide security status and trending across projects & across technology - SAST,DAST & SCA	10	Select	0	
34	The solution should employ the latest algorithms and techniques to ensure the most accurate testing and minimize false positives.	10	Select	0	
35	The solution provides role-based access control with the ability to maintain and enforce separation of duties between developers, security professionals, testers, managers etc.	10	Select	0	
36	The solution allows rule- or events-based trigger actions or notifications via SMTP.	10	Select	0	
37	The solution supports SSL and multiple LDAP servers.	10	Select	0	
38	The solution provides industry-standard single project and multiple-project reports.	10	Select	0	
39	The solution comes with the ability to create and customize additional reports.	10	Select	0	
40	The solution must support multiple common databases including Oracle, Microsoft SQL Server, MySQL	10	Select	0	
41	Should have feature to perform Auto Audit, to reduce manual audit time.	10	Select	0	
42	The solution must support deployment on-cloud license models.	10	Select	0	
43	Solution should allow for generating the custom reports.	10	Select	0	
44	Solution should be able to perform secret scanning	10	Select	0	
45	The solution supports a central dashboard for all the audit requirements and for governance needs & act as a collobration tool between Security & dev teams	10	Select	0	
46	The solution should be able to correalate common issues between SAST & DAST	10	Select	0	
47	Developers should be able to initiate the scans from IDEs and the scan should take place in a central server & also a provision to perform scan in Local IDE	10	Select	0	
48	Solution should support scanning the code only to find Critical and High level vulnerabilities	10	Select	0	
49	Solution should be able to exclude selected folders/files from the scan	10	Select	0	
50	Solution should not be licensed based on Number of application, should be capacity or concurrent scan based.	10	Select	0	
	Functional Specification - DAST				
51	The solution should have capability to scan web, mobile, API Security as well as single page applications.	10	Select	0	
52	The solution should be capable to perform scans on internal as well as external applications.	10	Select	0	
53	The solution should be capable to automate / schedule scans.	10	Select	0	
54	The solution should be capable to perform Black box as well as Grey box testing.	10	Select	0	

Application Security testing tool					
S.No	Required Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
55	The solution shall support simultaneous Crawl & Audit during scans. Or Crawl and test should happens in 2 phases. First the solution crawls and then tests This should helps in optimize the crawl data, remove any redundancy or duplicate pages to be tested in loop.	10	Select	0	
56	The solution shall allow for multiple concurrent scans.	10	Select	0	
57	The solution shall provide a built-in scan profiler to assist in tuning the scan configuration to a target server to improve the effectiveness and accuracy of the scan.	10	Select	0	
58	The solution allows for real-time review and investigation of vulnerabilities found while a test is still in progress.	10	Select	0	
59	The solution offers the capability to pause a scan for continuation later without the loss of data.	10	Select	0	
60	The solution offers the capability to schedule a single or multiple recurring scans in advance.	10	Select	0	
61	The solution has the capability to maintain false positive tags across scans	10	Select	0	
62	The solution supports Web Services security testing.	10	Select	0	
63	The solution provides REST/URL Rewriting (Variable) detection and support.	10	Select	0	
64	The solutions allow custom checks to be added	10	Select	0	
65	The solution comes with an array of out-of-the-box scan policies and all major compliance reports which may be further added to and customized.	10	Select	0	
66	The solution provides the ability to compare and report on two different scans to enable a delta analysis, including a visual representation of vulnerability differences between the two scans and the ability to drill-down into the differences.	10	Select	0	
67	The solution allows for a re-run of the entire scan with the same settings	10	Select	0	
68	The solution provides a shortcut to quickly re-test all vulnerabilities	10	Select	0	
69	The solution provides automatic vulnerability signature updates via the internet. Updates may also be performed manually for offline machines.	10	Select	0	
70	The solution integrates with a defect-tracking system for easy creation of defects from within the solution itself.	10	Select	0	
71	The solution has the capability to export scan data for upload to a web management console, to be correlated with security vulnerabilities found from static and interactive time testing. This offers a holistic view of the security status of applications and projects within an enterprise.	10	Select	0	
72	The solution shall have the ability to feed details of vulnerabilities found during a scan into Web Application Firewall and/or Intrusion Prevention Systems to block potential application exploits	10	Select	0	
73	The proposed solution must be able to record macros against Web 2.0 applications	10	Select	0	
74	The solution integrates and works out-of-the-box with a real-time application security technology within Java and .NET servers to: i Gather internal, code-level vulnerability information by observing the attacks in the code as they happen in real-time. ii Inspect parts of the application that it may not find through normal crawling. iii Collect information about the internal behaviours of a target application during dynamic tests. iv Detect new types of vulnerabilities, e.g., privacy violation and log fogging. v Provide stack trace and line-of-code detail during dynamic web application scanning.	10	Select	0	
75	Must support CAPTCHA/OTP/Composite Login process configuration in the proposed solution.	10	Select	0	
76	Solution should support 2FA/MFA authentication	10	Select	0	
77	Skip an attack while the scan is in progress.	10	Select	0	
78	Solution should support REST API SCAN and SOAP API Scan and support Swagger, ODATA, gRPC, GraphQL, SOAP, Postman data types for API Scan.	10	Select	0	
79	Solution should support Integration with other pen-testing tools.	10	Select	0	
80	View the actual attack during a scan session.	10	Select	0	

Application Security testing tool					
S.No	Required Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
81	Solution should generate rules to send to WAF.	10	Select	0	
82	The solution should also come with the Interactive Application Security Testing feature.	10	Select	0	
83	Integration with tools like POSTMAN and BURP.	10	Select	0	
84	Solution should support scanning only the vulnerabilities from previous scan, scan incremental, scan crawl and Audit from previous configurations	10	Select	0	
85	Solution should have the REST API to initiate/pause/stop/ scans and for various other functionalities	10	Select	0	
86	Should be able to scan and test a wide breath of application security vulnerabilities.	10	Select	0	
87	Should employ the latest algorithms and techniques to ensure the most accurate testing and minimize false positives.	10	Select	0	
88	The solution must be capable to generate report in following format: 1. The Title. 2. The Location (URL and/or line of code). 3. Specific vulnerability description. 4. Risk likelihood, business impact, and severity. 5. Specific remediation recommendations	10	Select	0	
89	Solution licensing should support concurrent/floating license	10	Select	0	
90	The solution should support OAST Vulnerability detection	10	Select	0	
91	The solution should support FAST proxy	10	Select	0	
92	The solution should support distributed scan sensors/agents to run the scans	10	Select	0	
TOTAL MARKS		920		0	

NOTE: Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or " Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product

DECOY						
S.No	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
1	Bidder must propose comprehensive deception solution which provides network, identity, cloud and critical infrastructure such as IT and IoT based decoy solution. Deception must have capability to build decoys, lures, and breadcrumbs.	RFP Requirement is applicable	10	Select	0	
2	Proposed solution must deploy deception capability by creating a fake environment to lure attackers into revealing themselves, to expose and eliminate threats early in the attack kill chain and prevent infected / suspicious user machine to connect with both wired and wireless network of the PSB infrastructure.	RFP Requirement is applicable	10	Select	0	
3	The proposed solution shall support applications, networks, and devices across data centre, DR, remote, and cloud environments. It shall support Decoy and Decoy Connector deployment across required segments, with scalability and customization as per Bank requirements, and shall not impose limits on Active Directory Decoy support.	RFP Requirement is applicable	10	Select	0	
4	Proposed solution must support lure mechanism beyond just decoy capability such as: - • Fake user credentials • Fake keys for cloud resources • Fake certificates • Fake document and template • Deception – SMB Token • Supports wide range of protocols(Includes IT/IIoT)	RFP Requirement is applicable	10	Select	0	
5	Decoy must support Detect Malware dropped onto Decoy, categorizing any websites visited from Decoys and In-depth malware analysis against malicious code. When a threat is detected, deception should assess the event severity.	RFP Requirement is applicable	10	Select	0	
6	On detecting suspicious activity, the deception platform sends captured files to the sandbox for analysis (in future), retrieves the results, and correlates them with the original event. This functionality to be provided out of the box or bidders must build required integration for same.	RFP Requirement is applicable	10	Select	0	
7	Proposed deception must support SOC integration where deception solution must allow: - i. Custom Dashboard on proposed SIEM. ii. SOAR Solution the ability to deploy, start, stop, delete, the decoy in deception solution. iii. Solution must provide out of the box capability to export IOC to be consumed by proposed SOC solutions.	RFP Requirement is applicable	10	Select	0	
8	Proposed solutions must have high interaction decoys with capability to have dynamic interactions, and as well as medium interaction decoys for Real-time engagement with attackers through emulated environments. Solution MUST have the ability to randomized decoy content (e.g., file names/types on SMB/SAMBA services) solution MUST have the ability for users to specific Decoy reset interval, to default to the state before any hacking attempts	RFP Requirement is applicable	10	Select	0	
9	Deployment capability:- • Should support Central Management for distributed Deployment. • Should support extension of Decoy from a central location to remote offices/location or cloud infrastructure. • Should support auto VLAN detection and addition to deployment networks. • Should support command line based approach for Decoy deployment	RFP Requirement is applicable	10	Select	0	
10	Should support to generate Deception Lure automatically for Decoy services, however, must support Safelist/trusted IPs to avoid False Positive alerts.	RFP Requirement is applicable	10	Select	0	
11	Decoy types of support, emulation of common network devices, including TCP port emulation. Network IT Decoys emulation of full OS Decoy supports real Operating Systems of Windows 7 / 10 / server 2016/2019, Linux, (Ubuntu/CentOS), SSLVPN, Business Applications/POS/DB/WEB, must support IT Decoys application with SWIFT LITE2, VPN Decoys	RFP Requirement is applicable	10	Select	0	
12	Eliminate External and Internal Attacks to/from decoys by identifying intrusions, malware, and website visits	RFP Requirement is applicable	10	Select	0	

DECOY						
S.No	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
13	Comprehensive reports from the incident alerts in PDF/CSV format, including a new alert engine that sends alerts over email based on your criteria.	RFP Requirement is applicable	10	Select	0	
14	Configure Alerts and send Alert Notifications via email, Common Event Format, and SYSLOG.	RFP Requirement is applicable	10	Select	0	
15	Should enable 2 factors for administrative logon	RFP Requirement is applicable	10	Select	0	
16	Should Integrate with LDAP/RADIUS/SAML remote admins	RFP Requirement is applicable	10	Select	0	
17	Solution should be provide RBAC for administrative access	RFP Requirement is applicable	10	Select	0	
18	The solution provides full visibility into the attacker's lifecycle mapped with MITRE ATTACK Framework. Tracks activities across decoys, enabling behavioral analysis and threat mapping.	RFP Requirement is applicable	10	Select	0	
19	The deception module generates actionable threat intelligence based on decoy interactions, with insights on attacker behaviors like botnet activity, frequent attacks, security scanner usage, and other IP attributes. Includes real-time traffic patterns (hourly, weekly, monthly) and detailed attack types (region-wise, ISP-wise, decoy-wise).	RFP Requirement is applicable	10	Select	0	
20	Includes an algorithm for automated rule creation that integrates with SOAR platforms, enabling real-time blocking of attacker IPs based on threat intelligence gathered from decoys. Features a customizable Generative AI model to assist security analysts with contextual insights, investigative support, and proactive security measures.	Includes an algorithm for automated rule creation that integrates with SOAR platforms, enabling real-time blocking of attacker IPs based on threat intelligence gathered from decoys. Features AI model to assist security analysts with contextual insights, investigative support, and proactive security measures.	10	Select	0	
21	Captures commands executed on high-interaction decoys with minimal performance impact, using agentless/agent mechanisms. Decoys feature self-deletion and self-triggering to remain undetected by attackers.	RFP Requirement is applicable	10	Select	0	
22	Offers Malware Analysis for malware captured via decoys or externally submitted samples. Includes static and dynamic analysis, reverse engineering, and behavior monitoring in a secure sandbox. Detailed reports include IOCs, persistence mechanisms, and containment recommendations.	RFP Requirement is applicable	10	Select	0	
23	The proposed solution shall provide an deception technology platform capable of deploying agentless and/or agent-based deception techniques to detect, delay, and identify unauthorized access, lateral movement, reconnaissance, credential theft, and malicious activities by presenting deceptive assets, services, credentials, and attack paths across the enterprise environment.	RFP Requirement is applicable	10	Select	0	
24	The proposed solution shall provide end-to-end visibility into attacker activities across the cyber kill chain and/or MITRE ATT&CK framework (or equivalent industry recognized framework), including behavioral analysis, attack path visualization, threat correlation, and forensic investigation.	RFP Requirement is applicable	10	Select	0	
25	The proposed solution shall be delivered as a cloud-based/SaaS platform hosted within the CSP environment. The bidder shall provision and size the required cloud compute, storage, network, and other platform resources to meet the Bank's performance, scalability, High Availability (HA), service continuity, and Disaster Recovery (DR) requirements in accordance with the applicable Cloud Deployment Model.	Deployment Mode: Cloud (SaaS) / Hybrid / On-premise Deployment Location: In case of Cloud/Hybrid: • At Bank's DC & DR: Any agent/Enforcer/Deceptor – Standalone at DC and Standalone at DR. • At Cloud (SaaS): Standalone Deployment aligned with the SLA (Refe Section 13). In case of On-premise: • At Bank's DC & DR: Standalone at DC and Standalone at DR.	10	Select	0	
26	The proposed solution shall support multiple types of decoys, emulation of commor network devices, including TCP port emulation. Network IT Decoys emulation of full OS Decoy supports real Operating Systems of Windows 7 / 10 / server 2016/2019 Linux, (Ubuntu/CentOS), ERP/POS/DB/WEB	The proposed solution shall support multiple types of decoys, emulation of common network devices, including TCP port emulation. Network IT Decoys emulation of full OS Decoy supports real Operating Systems like Windows, Linux, ERP/POS/DB/WEB etc.	10	Select	0	
27	The system must actively and passively detect Man-in-the-Middle (MITM) attacks and spoofing attempts, including mDNS, LLMNR, and NBT-NS	RFP Requirement is applicable	10	Select	0	
28	The proposed solution shall support high-interaction deception capabilities capable of securely recording attacker activities, commands, file access, and behavioral indicators for forensic analysis.	RFP Requirement is applicable	10	Select	0	
29	The proposed solution shall support integration with endpoint protection, anti-malware, IPS, NGFW, EDR/XDR, SIEM, SOAR, and other enterprise security solutions to correlate deception events with endpoint, network, and security telemetry.	RFP Requirement is applicable	10	Select	0	

DECOY						
S.No	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
TOTAL MARKS			290		0	

NOTE: Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or " Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must

Vulnerability Assessment & vulnerability lifecycle Management						
S.No	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
1	The proposed solution shall be deployable entirely on-premises and shall not require any cloud-hosted component, external service, or Internet connectivity for its core functionality, scanning, management, reporting, analytics, or product capabilities.	Clause stands deleted				
2	The proposed solution shall be available under perpetual and/or subscription licensing models.	RFP Requirement is applicable	10	Select	0	
3	The proposed solution shall be software-based and fully deployable on the hardware infrastructure proposed by the Bidder.	RFP Requirement is applicable	10	Select	0	
4	The proposed solution shall provide built-in dashboards and reporting capabilities with customizable templates.	RFP Requirement is applicable	10	Select	0	
5	The proposed solution shall incorporate secure-by-design architecture with built-in security mechanisms including authentication, encryption, audit logging, secure communication etc.	RFP Requirement is applicable	10	Select	0	
6	The proposed solution shall support vulnerability and configuration assessment across heterogeneous environments, including standard and customized operating systems, databases, network devices, virtualization platforms, containers, and supported firmware versions.	RFP Requirement is applicable	10	Select	0	
7	The proposed solution shall support configurable data retention, archival, and purging policies in accordance with the Bank's data retention requirements.	RFP Requirement is applicable	10	Select	0	
8	The proposed solution shall provide centralized Vulnerability Assessment and Vulnerability Management capabilities for discovery, assessment, prioritization, tracking, reporting, and remediation management across the Bank's entire IT infrastructure.	RFP Requirement is applicable	10	Select	0	
9	Each scanning engine shall support web application security assessment together with traditional infrastructure vulnerability and configuration/compliance assessment. The solution shall identify vulnerabilities, missing patches, insecure configurations, and compliance deviations, and generate comprehensive reports containing risk severity, evidence of findings, affected assets, and remediation recommendations to support security governance, audit, and regulatory compliance.	RFP Requirement is applicable	10	Select	0	
10	The proposed solution shall support deployment across physical, virtual, and containerized environments.	RFP Requirement is applicable	10	Select	0	
11	The proposed solution shall support deployment using industry-standard container technologies, including Docker or equivalent compliant container platforms.	RFP Requirement is applicable	10	Select	0	
12	The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and failover capabilities.	RFP Requirement is applicable	10	Select	0	
13	The proposed solution shall support centrally managed distributed scanning engines deployed across geographically dispersed locations.	RFP Requirement is applicable	10	Select	0	
14	The proposed solution shall support granular Role-Based Access Control (RBAC) based on users, roles, departments, business units, asset groups, and administrative functions.	RFP Requirement is applicable	10	Select	0	
15	The proposed solution shall support integration with SIEM, SOAR, Threat Intelligence Platforms, NAC, and other security platforms through APIs or standard integration mechanisms.	RFP Requirement is applicable	10	Select	0	
16	The proposed solution shall integrate with Privileged Access Management (PAM) solutions for secure credential management during authenticated scans.	RFP Requirement is applicable	10	Select	0	
17	The proposed solution shall integrate with IT Service Management (ITSM) and ticketing platforms for automated vulnerability tracking and remediation workflows.	RFP Requirement is applicable	10	Select	0	
18	The proposed solution shall support both active and passive asset discovery and vulnerability assessment/scanning.	RFP Requirement is applicable	10	Select	0	
19	The proposed solution shall support scan-less or telemetry-based vulnerability identification, where supported, to supplement conventional scanning techniques.	RFP Requirement is applicable	10	Select	0	
20	The proposed solution shall automatically discover, classify, inventory, and prioritize assets based on business criticality and security risk.	RFP Requirement is applicable	10	Select	0	
21	The proposed solution shall support authenticated and unauthenticated vulnerability assessments.	RFP Requirement is applicable	10	Select	0	

Vulnerability Assessment & vulnerability lifecycle Management						
S.No	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
22	The proposed solution shall prioritize vulnerabilities using CVSS, exploit availability, threat intelligence, asset criticality, business context, and risk-based scoring.	RFP Requirement is applicable	10	Select	0	
23	The proposed solution shall assess configuration compliance against industry standards, regulatory requirements, and Bank-defined security baselines.	RFP Requirement is applicable	10	Select	0	
24	The proposed solution shall support DHCP-based asset identification and tracking.	RFP Requirement is applicable	10	Select	0	
25	The proposed solution shall support intelligent and adaptive port discovery to optimize scan efficiency while minimizing network impact.	RFP Requirement is applicable	10	Select	0	
26	The proposed solution shall provide mechanisms to minimize, validate, suppress, and manage false-positive findings.	RFP Requirement is applicable	10	Select	0	
27	The proposed solution shall support both active and passive techniques for vulnerability detection, where applicable.	RFP Requirement is applicable	10	Select	0	
28	The proposed solution shall receive regular vulnerability intelligence and detection content updates, including newly disclosed vulnerabilities and security advisories.	RFP Requirement is applicable	10	Select	0	
29	The proposed solution shall support vulnerability assessment and compliance reporting aligned with PCI DSS requirements.	RFP Requirement is applicable	10	Select	0	
30	The proposed solution should provide predictive risk analysis or exploitability assessment based on vulnerability intelligence and threat context.	RFP Requirement is applicable	10	Select	0	
31	The proposed solution shall provide configurable dashboards, executive reports, operational reports, compliance reports, trend analysis, and scheduled report generation.	RFP Requirement is applicable	10	Select	0	
32	The proposed solution shall provide secure RESTful APIs or equivalent interfaces for integration and automation.	RFP Requirement is applicable	10	Select	0	
33	The proposed solution shall support deployment and lifecycle management of scanning agents without dependency on cloud-hosted services.	RFP Requirement is applicable	10	Select	0	
34	The proposed solution shall assess Active Directory security posture and identify misconfigurations, privilege risks, insecure policies, and exposure of critical directory services.	RFP Requirement is applicable	10	Select	0	
35	The proposed solution shall maintain a comprehensive and regularly updated vulnerability detection library covering a broad range of CVEs, security checks, compliance controls, and technology-specific plugins. The solution should support at aleast 200,000+ plugins and 75,000+ CVEs.	RFP Requirement is applicable	10	Select	0	
36	The solution shall support CVSS v4.0 in addition to CVSS v3.1 for vulnerability scoring and prioritization.	RFP Requirement is applicable	10	Select	0	
37	The solution shall correlate vulnerabilities using CVSS, EPSS, CISA Known Exploited Vulnerabilities (KEV), threat intelligence, asset criticality and exploit availability to generate a unified enterprise risk score.	RFP Requirement is applicable	10	Select	0	
38	The solution shall continuously discover managed, unmanaged, transient and rogue assets across the enterprise.	RFP Requirement is applicable	10	Select	0	
39	The solution shall automatically identify End-of-Life (EOL), End-of-Support (EOS) operating systems, firmware, applications and databases.	RFP Requirement is applicable	10	Select	0	
40	The solution shall perform authenticated configuration assessment against CIS Benchmarks, DISA STIG, SCAP, PCI DSS and organization-defined baselines.	RFP Requirement is applicable	10	Select	0	
41	The solution shall support vulnerability assessment of Windows, Linux, UNIX, Network Devices, Databases, Hypervisors, Storage Systems and Virtual Appliances.	RFP Requirement is applicable	10	Select	0	
42	The solution shall support vulnerability assessment of VMware ESXi, Hyper-V, Nutanix AHV, Kubernetes, OpenShift and container platforms.	RFP Requirement is applicable	10	Select	0	
43	The solution shall support assessment of network devices including firewalls, routers, switches, wireless controllers, VPN gateways and load balancers.	RFP Requirement is applicable	10	Select	0	
44	The solution shall automatically validate remediation through scheduled or on-demand re-scanning and maintain complete remediation history.	RFP Requirement is applicable	10	Select	0	
45	The solution shall integrate with enterprise CMDB, ITSM, SIEM, SOAR, PAM and NAC platforms through secure REST APIs.	The solution shall integrate with enterprise CMDB, ITSM, SIEM, SOAR, PAM and NAC platforms.	10	Select	0	
46	The solution shall provide immutable audit trails for all administrative actions, scan activities, policy modifications and user access.	RFP Requirement is applicable	10	Select	0	

Vulnerability Assessment & vulnerability lifecycle Management						
S.No	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
47	The solution shall support Multi-Factor Authentication (MFA), LDAP, Active Directory, SAML 2.0 and OpenID Connect authentication.	RFP Requirement is applicable	10	Select	0	
48	The solution shall support secure encrypted communication using TLS 1.3 and cryptographic modules compliant with FIPS 140-3 or equivalent internationally recognized standards.	The solution shall support secure encrypted communication using TLS 1.3 and cryptographic modules compliant with FIPS 140-2/FIPS 140-3 or equivalent internationally recognized standards.	10	Select	0	
49	The solution shall support offline signature and plugin updates for deployment in isolated or air-gapped environments.	RFP Requirement is applicable	10	Select	0	
50	The solution shall verify the integrity and authenticity of vulnerability plugins, signatures and update packages using digitally signed updates.	RFP Requirement is applicable	10	Select	0	
51	The solution shall identify internet-facing assets and continuously monitor externally exposed services.	Clause stands deleted				
52	The solution shall support asset tagging based on business unit, application, owner, location, criticality and regulatory classification.	RFP Requirement is applicable	10	Select	0	
53	The solution shall support vulnerability assessment for IPv4 and IPv6 environments.	RFP Requirement is applicable	10	Select	0	
54	The solution shall provide executive, operational and technical dashboards with drill-down capability and customizable KPIs.	RFP Requirement is applicable	10	Select	0	
55	The solution shall support scheduled, event-driven and API-triggered vulnerability scans.	RFP Requirement is applicable	10	Select	0	
56	The solution shall support digitally signed and password-protected reports with configurable retention and archival.	The solution shall support digitally signed/password-protected reports with configurable retention and archival.	10	Select	0	
57	The solution shall support detection of weak SSL/TLS configurations, deprecated protocols, insecure cipher suites and certificate misconfigurations.	RFP Requirement is applicable	10	Select	0	
58	The solution shall identify weak authentication mechanisms including default credentials, weak password policies and insecure authentication configurations.	RFP Requirement is applicable	10	Select	0	
59	The solution shall support secure credential management through integration with enterprise Privileged Access Management (PAM) solutions without storing privileged credentials in clear text.	RFP Requirement is applicable	10	Select	0	
60	The solution shall provide comprehensive REST APIs and webhook support for automation and integration with enterprise security platforms.	The solution shall provide comprehensive APIs or webhook support for automation and integration with enterprise security platforms.	10	Select	0	
61	The solution shall support CVSS v3.1 and/or CVSS v4.0 for vulnerability scoring and prioritization and shall support newer CVSS versions as they become generally available.	RFP Requirement is applicable	10	Select	0	
62	The solution shall correlate vulnerabilities using CVSS, threat intelligence, exploit intelligence, asset criticality, business context, and, where supported, industry-recognized exploit prediction methodologies (e.g., EPSS), Known Exploited Vulnerability (KEV) intelligence, or equivalent intelligence sources to generate a unified enterprise risk score.	RFP Requirement is applicable	10	Select	0	
63	The solution shall support continuous or scheduled discovery of managed, unmanaged, transient, rogue, and network-connected assets using active, passive, agent-based, or equivalent discovery mechanisms.	RFP Requirement is applicable	10	Select	0	
64	The solution shall identify End-of-Life (EOL), End-of-Support (EOS), obsolete, or unsupported operating systems, firmware, applications, and databases using OEM lifecycle information, vulnerability intelligence, or equivalent mechanisms.	RFP Requirement is applicable	10	Select	0	
65	The solution shall perform authenticated configuration assessment against industry-recognized security benchmarks including CIS Benchmarks, PCI DSS, SCAP, DISA STIG (where supported), and Bank-defined security baselines.	RFP Requirement is applicable	10	Select	0	
66	The solution shall support vulnerability assessment of Windows, Linux, UNIX, Network Devices, Databases, Hypervisors, Storage Systems and Virtual Appliances.	RFP Requirement is applicable	10	Select	0	
67	The solution shall support vulnerability assessment of virtualization platforms (including VMware ESXi, Hyper-V, Nutanix AHV or equivalent where supported), container platforms, and orchestration platforms such as Kubernetes, OpenShift, or equivalent technologies.	RFP Requirement is applicable	10	Select	0	
68	The solution shall support assessment of network devices including firewalls, routers, switches, wireless controllers, VPN gateways and load balancers.	RFP Requirement is applicable	10	Select	0	

Vulnerability Assessment & vulnerability lifecycle Management						
S.No	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
69	The solution shall automatically validate remediation through scheduled or on-demand re-scanning and maintain complete remediation history.	RFP Requirement is applicable	10	Select	0	
70	The solution shall integrate with enterprise CMDB, ITSM, SIEM, SOAR, PAM, NAC, and equivalent enterprise platforms through secure REST APIs and/or standard integration mechanisms.	RFP Requirement is applicable	10	Select	0	
71	The solution shall provide tamper-evident or immutable audit trails for all administrative actions, scan activities, policy modifications, and user access, and support forwarding of audit logs to centralized log management or SIEM platforms.	RFP Requirement is applicable	10	Select	0	
72	The solution shall support Multi-Factor Authentication (MFA) and enterprise authentication mechanisms	RFP Requirement is applicable	10	Select	0	
73	The solution shall support secure encrypted communication using TLS 1.3 and cryptographic modules compliant with FIPS 140-2, FIPS 140-3, or equivalent internationally recognized cryptographic standards, as applicable.	For Fully On-premise : The solution shall be deployed within the Bank's on-premise environment and shall support authenticated/credentialed vulnerability assessment of the Bank's internal infrastructure, including servers, network devices, databases, virtual machines, applications, and other supported assets or For SaaS Cloud with On-premise component: The solution shall support authenticated/credentialed vulnerability assessment of the Bank's on-premise infrastructure through a dedicated scanning appliance, sensor, or agent deployed within the Bank's network. The on-premise scanning component shall securely communicate with the SaaS platform over encrypted communication using TLS 1.2 or higher, preferably TLS 1.3, and shall support outbound-only communication from the Bank's network without requiring inbound access from the SaaS platform. The solution shall securely store, manage, and utilize scanning credentials using industry-standard encryption and appropriate access controls. Cryptographic modules used for the protection of scanning credentials and sensitive data shall be FIPS 140-2/FIPS 140-3 compliant. Scanning credentials shall be securely stored and utilized within the Bank's controlled environment and shall not be exposed to or transmitted to the SaaS platform The proposed VA/VLM solution shall use industry-standard cryptographic mechanisms and secure cryptographic modules for the protection of all credentials, passwords, API keys, tokens, certificates, and other secrets stored within the solution	10	Select	0	
74	The solution shall support offline signature and plugin updates for deployment in isolated or air-gapped environments.	RFP Requirement is applicable	10	Select	0	
75	The solution shall verify the integrity and authenticity of vulnerability plugins, signatures and update packages using digitally signed updates.	RFP Requirement is applicable	10	Select	0	
76	The solution shall identify internet-facing assets and externally exposed services through native capabilities and/or integration with External Attack Surface Management (EASM) or equivalent solutions	RFP Requirement is applicable	10	Select	0	
77	The solution shall support asset tagging based on business unit, application, owner, location, criticality and regulatory classification.	RFP Requirement is applicable	10	Select	0	
78	The solution shall support vulnerability assessment for IPv4 and IPv6 environments.	RFP Requirement is applicable	10	Select	0	
79	The solution shall provide executive, operational and technical dashboards with drill-down capability and customizable KPIs.	RFP Requirement is applicable	10	Select	0	
80	The solution shall support scheduled, event-driven and API-triggered vulnerability scans.	RFP Requirement is applicable	10	Select	0	
81	The solution shall support password-protected and/or digitally signed reports with configurable retention and archival.	RFP Requirement is applicable	10	Select	0	
82	The solution shall support detection of weak SSL/TLS configurations, deprecated protocols, insecure cipher suites and certificate misconfigurations.	RFP Requirement is applicable	10	Select	0	
83	The solution shall identify weak authentication mechanisms including default credentials, weak password policies and insecure authentication configurations.	RFP Requirement is applicable	10	Select	0	

Vulnerability Assessment & vulnerability lifecycle Management						
S.No	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
84	The solution shall support secure credential management through integration with enterprise Privileged Access Management (PAM) solutions without storing privileged credentials in clear text.	RFP Requirement is applicable	10	Select	0	
85	The solution shall provide comprehensive REST APIs and/or standard integration interfaces including Webhooks, Syslog or equivalent mechanisms for automation and integration with enterprise security platforms.	RFP Requirement is applicable	10	Select	0	
86	The proposed solution shall provide a centralized and correlated view of vulnerability findings identified across supported assessment sources, including network, host, server, endpoint, cloud, container, database, and device configuration assessments. The solution shall normalize findings into a common format to enable centralized analysis, deduplication, correlation, risk-based prioritization, remediation tracking, and reporting.	RFP Requirement is applicable	10	Select	0	
87	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	Clause stands deleted				
88	Unified, correlated findings intelligence. Every scanning engine — across web, API, network and host, cloud, containers, mobile, source code, device configuration and identity — reports into a single normalized findings model. .	RFP Requirement is applicable	10	Select	0	
89	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	Clause stands deleted				
90	Mobile Application Security Testing: The proposed solution shall support static security analysis of Android and iOS mobile application packages, including APK/AAB and IPA formats, and shall provide security assessment mapped to recognized mobile application security standards and methodologies such as OWASP MASVS and MASTG.	RFP Requirement is applicable	10	Select	0	
91	White-Label Reporting and Approval Workflow: The proposed solution shall support customizable/white-label security assessment reports, including organization-specific branding and configurable report content. The solution shall support role-based maker-checker workflow for report generation, review, approval, and controlled release of finalized reports.	White-Label Reporting and Approval Workflow: The proposed solution shall support customizable/white-label security assessment reports, including organization-specific branding and configurable report content. The solution shall support role-based or maker-checker workflow for report generation, review, approval of finalized reports.	10	Select	0	
92	Multi-Tenant Data Isolation: The proposed solution shall support secure multi-tenancy for managed-security/shared-service deployments, providing logical and access-controlled segregation of each customer's assets, credentials, scan configurations, findings, reports, and other security data. APIs and administrative interfaces shall enforce appropriate tenant-level authorization and data isolation.	Clause stands deleted				
93	Remediation Tracking and Risk Trends: The proposed solution shall provide comparison of assessment results across multiple scan cycles and identify vulnerabilities that are newly discovered, remediated/fixed, recurring, or persistent. It shall provide asset-level remediation tracking and risk trends over time to demonstrate improvement in the security posture.	RFP Requirement is applicable	10	Select	0	

Vulnerability Assessment & vulnerability lifecycle Management						
S.No	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
94	Secure Credential Management for Authenticated Scanning: The proposed solution shall support secure, temporary, and controlled provisioning of credentials required for authenticated vulnerability assessments to distributed scanning components. Credentials shall not be retained in plaintext or stored as persistent privileged credentials on distributed scan nodes. The solution shall support secure credential transmission and mechanisms such as mutual authentication, short-lived credentials, credential leasing, or equivalent controls to minimize the risk of credential exposure and standing privileged access.	RFP Requirement is applicable	10	Select	0	
TOTAL MARKS			890		0	

NOTE: Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or " Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product

Idendity Threat Detection and Response (ITDR)						
S.No	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
1	Identity Threat Detection & Response					
1.1	Identity Threat Detection solution can be proposed as either a single solution or combiniation of multiple of solution	RFP Requirement is applicable	10	Select	0	
1.2	Identity Threat Detection Solution should Identify currently vulnerable identities and associated credentials that would provide an attack path to an attacker post initial compromise.	RFP Requirement is applicable	10	Select	0	
1.3	Identity Threat Detection Solution should make vulnerable identities data available as context to systems that track the most highly attacked and privileged people in the organization.	RFP Requirement is applicable	10	Select	0	
1.4	Identity Threat Detection Solution must find and present high-risk attack pathways to critical IT assets	Present identity risk attack pathways/ context to critical IT assets.	10	Select	0	
1.5	Identity Threat Detection Solution must uncover forgotten connections and errant credentials that facilitate attacker mobility	RFP Requirement is applicable	10	Select	0	
1.6	Identity Threat Detection Solution should must automatically prioritize and remediate the riskiest identities to preemptively cut off what attackers need (and expect to find) to move undetected within the network.	Identity Threat Detection Solution should must automatically prioritize and remediate the riskiest identities within the network.	10	Select	0	
1.7	Identity Threat Detection Solution Should detect and respond to active threats with high fidelity (low false positives and false negatives).	RFP Requirement is applicable	10	Select	0	
1.8	Identity Threat Detection Solution should provide contextual information—who, what, when and how—to inform all stages of the attack chain.	RFP Requirement is applicable	10	Select	0	
1.9	Identity Threat Detection Solution should provide deep insights into both the potential and used privilege escalation and lateral movement steps in an attack.	RFP Requirement is applicable	10	Select	0	
2	Active Directory Vulnerability Discovery and Remediation					
2.1	Identity Threat Detection Solution should discover and provide/suggest remediation for, insufficient or improper PAM configuration and management of service-account, local-administrator, and privileged-domain credentials	RFP Requirement is applicable	10	Select	0	
2.2	Identity Threat Detection Solution should discover and provide/suggest remediation for, unintentional creation of shadow admin accounts that have excessive privileges	RFP Requirement is applicable	10	Select	0	
2.3	The ITDR solution shall identify and assess exposed, improperly stored, or compromised credentials associated with user, privileged, service, and administrative identities on endpoints	The ITDR solution shall identify and assess exposed, improperly stored, or compromised credentials associated with user, privileged, service, and administrative identities/accounts.	10	Select	0	
2.4	Identity Threat Detection Solution should Identify, Misconfigured accounts, Legacy app accounts, Stale accounts, password policy violations, Kerberoastable credentials, unmanaged user accounts, unmanaged service accounts	Identity Threat Detection Solution should Identify, Misconfigured accounts, Stale accounts, password policy violations, Kerberoastable credentials.	10	Select	0	
2.5	Identity Threat Detection Solution should Provide continuous monitoring and customizable, automated business rules to eliminate security policy violations, such as: • Stored credentials to sensitive assets • Local-admin accounts • Cached credentials stored in browsers, Windows and other systems	Identity Threat Detection Solution should Provide continuous monitoring and customizable, automated business rules to eliminate security policy violations, such as: • Stored credentials to sensitive assets • Privileges modifications • Suspicious identity activity	10	Select	0	
2.6	Identity Threat Detection Solution should be capable of creating tickets in the organization's ITSM system for vulnerabilities that cannot be safely addressed through automation, allowing them to be managed and remediated through established IT operational workflows.	Clause Stands Deleted				
2.7	Identity Threat Detection Solution should be available through rack-mountable on-premise deployment	Clause Stands Deleted				
2.8	Identity Threat Detection Solution should provide a GUI for user to control the applications.	RFP Requirement is applicable	10	Select	0	
2.9	Identity Threat Detection Solution should detect all types of attack vectors including but not limited to pre attack reconnaissance,zero- day attacks, privilege escalation prevention, lateral movement, data theft	RFP Requirement is applicable	10	Select	0	
2.10	Identity Threat Detection Solution should detect multiple attacks simultaneously.	RFP Requirement is applicable	10	Select	0	
2.11	Identity Threat Detection Solution should discover vulnerable identities, exposures and misconfigurations	RFP Requirement is applicable	10	Select	0	
2.12	Identity Threat Detection Solution should provide insight into how a combination of these vulnerabilities can provide attack paths to crown jewel IT assets or other critical or sensitive systems	RFP Requirement is applicable	10	Select	0	
2.13	Identity Threat Detection Solution should present attack paths and how to remediate them in an actionable and visually effective way	RFP Requirement is applicable	10	Select	0	

Idendity Threat Detection and Response (ITDR)						
S.No	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
2.14	Identity Threat Detection controls should begin with understanding what IT systems are a priority to protect.	RFP Requirement is applicable	10	Select	0	
2.15	Identity Threat Detection controls should be able to automatically discover and flag hidden or shadow Tier 0 assets	Identity Threat Detection controls should be able to automatically discover and flag privileges changes, exposure across identity.	10	Select	0	
2.16	Identity Threat Detection Solution should be able to discover identity vulnerabilities and their relationship to each other and the organization's crown jewel IT assets	RFP Requirement is applicable	10	Select	0	
2.17	Identity Threat Detection Solution should be able to pull and analyze identity data from AD, Entra ID, identity stores, PAM systems	Identity Threat Detection Solution should be able to pull and analyze identity data from identity sources i.e., Active Directory and Microsoft Entra ID.	10	Select	0	
2.18	Identity Threat Detection Solution should integrate with the organization's ITSM and software distribution systems to facilitate the collaboration between security and IT teams	Clause Stands Deleted				
3	**AD Threat Detection and Response**					
3.1	Identity Threat Detection Solution should be capable of creating tickets in the organization's ITSM system for vulnerabilities that cannot be safely addressed through automation, allowing them to be managed and remediated through established IT operational workflows. not require the deployment of a persistent agent	RFP Requirement is applicable	10	Select	0	
3.2	Identity Threat Detection Solution should provide the unified presentation of both source- and target-based telemetry data in a timeline view.	RFP Requirement is applicable	10	Select	0	
3.3	The ITDR solution shall support correlation of identity-related telemetry from relevant source and target systems to identify and investigate identity compromise, privilege escalation, credential abuse, and lateral movement.	RFP Requirement is applicable	10	Select	0	
3.4	The Identity Threat Detection Solution should integrate with compatible endpoint/extended detection solution to capture screen recordings or screenshots during active attacker sessions, as part of advanced forensic evidence collection	Clause Stands Deleted				
3.5	The Identity Threat Detection Solution should integrate with compatible network detection solution to support collection of PCAP data to support network-level visibility of the incident	Clause Stands Deleted				
3.6	Identity Threat Detection Solution should push incident data into other technologies such as SIEM/XDR or SOARs via integrations for improved incident management.	RFP Requirement is applicable	10	Select	0	
3.7	Identity Threat Detection Solution should, as part of its forensic data collection process, include detailed attack path information, including the protocols leveraged during the attack.	Identity Threat Detection Solution, as part of data collection process, should include detailed attack path information, the protocols/process details leveraged during the attack etc.	10	Select	0	
3.8	Identity Threat Detection Solution should collect user and computer information from Active Directory as part of its forensic data gathering to enhance context and assess risk exposure.	Identity Threat Detection Solution should collect user and computer information from Active Directory as part of data gathering to enhance context and assess risk exposure.	10	Select	0	
3.9	Identity Threat Detection solution should detect an adversary's attempt to move laterally toward the organization's key assets using as many hosts (Windows, Mac, or Linux) as possible in the organization without requiring a persistent agent.	Identity Threat Detection solution should detect an adversary's attempt to move laterally toward key assets using as many hosts (Windows, Mac or Linux) as possible.	10	Select	0	
3.10	Identity Threat Detection Solution should collect user and computer information from Active Directory as part of its forensic data gathering to enhance context and assess risk exposure. detect at the earliest point in the attack, post initial compromise as the attacker is first attempting to move laterally and escalate privilege.	Identity Threat Detection Solution should collect user and computer information from Active Directory as part of data gathering to enhance context and assess risk exposure. Detect at the earliest point in the attack (like compromised accounts, privilege escalation, anomalous access), post initial compromise as the attacker is first attempting to move laterally and escalate privilege.	10	Select	0	
3.11	Identity Threat Detection Solution should collect user and computer data from Active Directory during forensic data gathering to improve context and evaluate risk exposure, while ensuring that all deception techniques remain hidden from legitimate users.	Identity Threat Detection Solution should collect user and computer data from Active Directory during data gathering to improve context and evaluate risk exposure.	10	Select	0	
4	**General**					
4.1	The Identity Threat Detection and Response (ITDR) solution shall provide comprehensive detection, risk assessment, investigation and response capabilities for threats involving human and supported non-human identities, including user accounts, privileged accounts, service accounts and other supported identities, and shall correlate identity, authentication, access, privilege and behavioural activities to identify compromised, exposed, risky or misused identities.	RFP Requirement is applicable	10	Select	0	

Idendity Threat Detection and Response (ITDR)						
S.No	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
4.2	The ITDR solution shall provide identity threat detection, risk analysis and investigation across hybrid and cloud identity environments, including on-premises Active Directory, cloud identity providers, federated identities, SaaS applications and other supported identity sources, and shall correlate identity-related risk and activity across connected environments.	RFP Requirement is applicable	10	Select	0	
4.3	The ITDR solution shall establish continuously updated behavioural risk profiles for supported identities and shall identify anomalous or materially deviating patterns involving authentication, access, privilege, device, application, location, time and resource usage, and shall provide contextual risk scoring to support identification and prioritization of potentially compromised or high-risk identities.	RFP Requirement is applicable	10	Select	0	
4.4	The ITDR solution shall provide continuously updated identity risk assessment and relationship analysis across identities, accounts, groups, privileges, devices, applications and critical resources, and shall identify risky relationships and combinations of exposures that may facilitate identity compromise, privilege escalation or lateral movement.	RFP Requirement is applicable	10	Select	0	
4.5	The ITDR solution shall support policy-controlled response and risk mitigation for identified identity threats, including restricting or disabling risky identities, initiating credential remediation, enforcing additional authentication controls and invoking integrated security controls, as supported by the connected identity platforms and configured Bank policies.	RFP Requirement is applicable	10	Select	0	
TOTAL MARKS			380		0	

NOTE: Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or " Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available

Cloud Security						
S.No	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
The OEM shall submit mandatory compliance with the Cloud Deployment requirements along with the						
1	The solution must support major cloud provider like AWS, Azure, Google Cloud). For all supported cloud providers, the supported solution must support ○ Agentless Scanning ○ Full audit trails of the solution ○ Granular RBAC based on account / subscription /project or custom grouping	RFP Requirement is applicable	10	Select	0	
2	The solution must provide a detailed inventory of all assets/resources including but not limited to the following ○Resource type ○Configuration ○Identity Access management (User, Role, Group, etc) ○IAM permission (All, Used, Excessive) ○External Identity Store	RFP Requirement is applicable	10	Select	0	
3	The solution must detect misconfiguration related to IAM, compute, network data, security etc across multi-cloud environments and provide step-by-step remediation recommendations.	RFP Requirement is applicable	10	Select	0	
4	The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud envirionment like AWS/Azure/GCP/Meghdoot, AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.	The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud environment like AWS/Azure/GCP, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.	10	Select	0	
5	The solution must be able to identify publicly exposed resources across multi-cloud environments including identities, cross-account and data resources	RFP Requirement is applicable	10	Select	0	
6	The solution must provide full visibility into multi-cloud keys, secrets, certificates, access keys and their entitlements. The solution should also detect publicly exposed keys and secrets, cleartext secrets stored in environment variables, VM startup scripts, tags, configuration, etc	RFP Requirement is applicable	10	Select	0	
7	The solution must support API-based integration with Identity providers for full visibility into cloud entitlements including excessive permissions.	RFP Requirement is applicable	10	Select	0	
8	The solution must provide Identity risk governance including but not limited to the following ○Cloud provider-centric identities and entitlements visibility ○Visibility of all, used and excessive permission/privilege ○Visibility of federated identities ○Identify inactive, 3rd party, users and service identities, MFA status, static credentials ○Provide least privilege permission ○Automatic detection of anomalous behavior	RFP Requirement is applicable	10	Select	0	
9	The solution must analyze the effective privileges and provide the Least Privilege recommendations for the following scenarios ○ Analyze effective usage of permissions based on activity, including awareness to unlogged actions, complex scenarios ○ Detect and remediate inactive identities (human, machine, federated users) ○ Detect cloud-native identities with excessive (unused) permissions ○ Detect federated identities with excessive (unused) permissions ○ Evaluate the risk of excessive permissions for each identity, resource, or deployment scope (e.g., account, subscription) ○ Provide least-privilege recommendations for cloud-native identities (including 3rd parties)- e.g. AWS SSO permission sets ○ Provide least-privilege recommendations for federated identities ○ Create resource-granular least-privilege recommendations in cloud-native language (e.g. JSON, Terraform) ○ Automatic, in-product remediation via the Cloud Service Provider (CSP) API (1-click) ○ Detect and visualize entitlements to data stores ○ Detect public and cross-account data stores ○ Automatically label/tag sensitive data stores ○ Limit access to sensitive resources via least-privilege policy recommendations ○ Detect misconfigured data stored (e.g. encryption, key rotation) ○ Detect unusual access to data (anomaly detection) ○ Least-privilege recommendations for resource-based configuration (e.g. S3 bucket policies)	The solution must analyze the effective privileges and provide the Least Privilege recommendations for the following scenarios ○ Analyze effective usage of permissions based on activity, including awareness to unlogged actions, complex scenarios ○ Detect and remediate inactive identities (human, machine, federated users) ○ Detect cloud-native identities with excessive (unused) permissions ○ Detect federated identities with excessive (unused) permissions ○ Evaluate the risk of excessive permissions for each identity, resource, or deployment scope (e.g., account, subscription) ○ Provide least-privilege recommendations for cloud-native identities (including 3rd parties)- e.g. AWS SSO permission sets ○ Provide least-privilege recommendations for federated identities ○ Create resource-granular least-privilege recommendations in cloud-native language (e.g. JSON, Terraform) ○ Automatic, in-product remediation. ○ Detect and visualize entitlements to data stores ○ Detect public and cross-account data stores ○ Automatically label/tag sensitive data stores ○ Limit access to sensitive resources via least-privilege policy recommendations ○ Detect misconfigured data stored (e.g. encryption, key rotation) ○ Detect unusual access to data (anomaly detection) ○ Least-privilege recommendations for resource-based configuration (e.g. S3 bucket policies)	10	Select	0	
10	Solution must provide role based access control for cloud (Public/Private) environment	RFP Requirement is applicable	10	Select	0	
11	The solution must create an inventory of Network resources and configurations, detect misconfiguration and create a network path visualization of publicly exposed resources. It also should differentiate between direct and indirect exposure & wide vs restricted network exposure	RFP Requirement is applicable	10	Select	0	
12	The solution must have the ability to scan cloud workloads (VMs and containers) to detect vulnerabilities and create a toxic combination if it is exposed to the internet or higher privileges.	RFP Requirement is applicable	10	Select	0	

Cloud Security						
S.No	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
13	The solution must have the ability to correlate workload misconfiguration/vulnerability to the impacted resource template (eg. Launch template, auto scaling group, etc)	RFP Requirement is applicable	10	Select	0	
14	The solution must have the ability to provide vulnerability remediation prioritization based on the attack vector, known exploit status, etc	RFP Requirement is applicable	10	Select	0	
15	The solution must discover and detect misconfigurations of Kubernetes clusters (GKE, AKS, EKS) and evaluate against common security benchmarks (e.g. CIS)	RFP Requirement is applicable	10	Select	0	
16	The solution must provide visibility into K8s users, service accounts, effective permissions and cloud entitlements granted to K8s service accounts.	RFP Requirement is applicable	10	Select	0	
17	The solution must provide correlation of the runtime container with container repository, cluster, node and workload.	RFP Requirement is applicable	10	Select	0	
18	The solution must have to ability to scan IaC templates (e.g Terraform, CloudFormation templates) by integrating with CI/CD pipeline tools & source code repositories and should automatically generate least privilege recommendations in Terraform/CloudFormation templates	RFP Requirement is applicable	10	Select	0	
19	The solution must provide Investigation and Forensics features across multiple cloud providers, including source identity and activities performed by federated identities.	RFP Requirement is applicable	10	Select	0	
20	The solution must provide UEBA based Anomaly Detection by monitoring all access activities & API calls and must detect suspicious data access, privilege escalation, behavioral analysis etc	RFP Requirement is applicable	10	Select	0	
21	The solution must provide risk-based prioritization evaluating full environmental context and must provide built-in security findings management (e.g. exclude, resolve, snooze)	RFP Requirement is applicable	10	Select	0	
22	The solution must have the ability to resolve cloud misconfiguration findings via cloud-native APIs	RFP Requirement is applicable	10	Select	0	
23	The solution must support integration and automation with collaboration tools, SIEM tools, ITSM tools (Manage Engine) and customizable workflows through webhook triggers.	RFP Requirement is applicable	10	Select	0	
24	The solution must support querying platform data via API.	RFP Requirement is applicable	10	Select	0	
25	The solution must provide an self-service portal for engineers. The admin portal should be able to define the eligibility for users and groups, based on role, scope and duration. The solutuon should provide approval workflow and audit logs	The solution should have a Role based access system where user can login and update their system generated passwords, if required. Admin have rights to create the role based access controls and workflows with audit logs.	10	Select	0	
26	The propose solution should have Cloud Native Application Protection (CNAPP) as inbulit solution or additional solution that can provide security through a deep technological integration and strategic business alliance, delivering holistic security solution.	Clause Stand Deleted				
27	The proposed CNAPP solution should provides bank with more context to drive actionable security and smarter prevention, from code-to-cloud, across the application lifecycle.	Clause Stand Deleted				
28	The proposed CNAPP solution should must have below capabilities and required licenses from day one > CSPM - Compliance and governance for the full cloud stack > CIEM - Least Privildge Access/Excessive Permission and Identity Management > CWP - Protection/Response across all the running cloud workloads > KSPM - Container Security and compliance in the cloud and on-prem > CDR - detect, analyse and respond across the cloud environment > AISPM - Visbility and security for AI workloads, services and data used in training and inference >CTEM -- Continuous Threat Exposure Management (CTEM)	Clause Stand Deleted				
TOTAL MARKS			250		0	

NOTE: Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or " Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made

Threat Inteligence Platform (TIP)					
S.No	Required Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
The OEM shall submit mandatory compliance with the Cloud Deployment requirements along with the Functional Specifications of the proposed solution.					
	GENERAL				
1	The platform must have a long history with extensive historical data and deeper understanding of long - term threats trends and adversary evolution.	10	Select	0	
2	The platform must have the ability to add NLP/AIML to the platform as an add-on feature/in-built feature.	10	Select	0	
3	The platform must be able to provide intel Analytics.	10	Select	0	
4	The solution should integrate up to multiple sources of threat intelligence required by the organization into a single management platform without any extra cost. The Sources should either be part of the Intelligence Channels, or Commercial sources that the client is subscribed to.	10	Select	0	
5	The proposed solution shall provide a managed cloud-based platform for OSINT and third-party intelligence collection, aggregation, and processing, with minimal maintenance and management requirements from the Bank.	10	Select	0	
6	The solution should allow easy linking between all relevant threat data, such as atomic IOCs, campaigns, actors, and TTPs.	10	Select	0	
7	The solution should provide the ability to search all intelligence held on the platform from a single search string and/or using filter options and/or with customizable dashboards	10	Select	0	
8	The solution should assist the organization's threat analysts by providing managed threat analytics algorithms to provide a high accuracy confidence score on new threat intelligence with no configuration required and automated by AI.	10	Select	0	
9	The platform must be able to provide capability to create custom dashboards and Visualizations.	10	Select	0	
10	TIP Solution should have an out-of-the-box Threat Intelligence Playbook library for the following threat intel-based use cases such as IOC hunting, IOC Dissemination, IOC to Vulnerability mapping etc. OR TIP Solution should support out-of-the-box integration with third party solution* to create Threat Intelligence Playbook library for the following threat intel based use cases such as IOC hunting, IOC Dissemination, IOC to Vulnerability mapping etc. *In case third party solution is required, bidder to propose & provide the same along with the integration at no additional cost to the bank. Details shall be included as a part of the proposal.	10	Select	0	
11	Solution should be able to support reliable, actionable feeds for:				
11.1	IP Addresses	10	Select	0	
11.2	Domain Names	10	Select	0	
11.3	Hashes	10	Select	0	
11.4	E-Mails	10	Select	0	
11.5	File Names	10	Select	0	
11.6	Blacklists	10	Select	0	

Threat Inteligence Platform (TIP)					
S.No	Required Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
11.7	Malware Indicators	10	Select	0	
11.8	ASN	10	Select	0	
11.9	Mutex	10	Select	0	
11.10	Win Registry Key	10	Select	0	
11.11	Port	10	Select	0	
11.12	HTTP Session Object	10	Select	0	
11.13	User-Agent	10	Select	0	
11.14	Proposed solutionshould include the following elements in the IOC:	10	Select	0	
11.15	Source information (IP, Domain, URL etc.)	10	Select	0	
11.16	File formats (.exe, .doc, .pdf, .xml etc.)	10	Select	0	
11.17	Geo Location	10	Select	0	
11.18	File hash values	10	Select	0	
11.19	Vulnerability details	10	Select	0	
	FUNCTIONAL - DATA INGEST				
12	The solution should manage multiple feeds of data and ingest the aggregate of data into one set of usable data.	10	Select	0	
13	The solution should offer a wide range of free OSINT feeds out of the box, with no configuration effort	10	Select	0	
14	The solution should offer a wide range of commercial CTI providers out of the box, including atomic IOCs, threat bulletins, and any other threat intelligence offered by each provider.	10	Select	0	
15	The solution should support parsing intelligence from unstructured reports, STIX files and paste of data from another source.	10	Select	0	
16	The platform should be able to do the following to the CTI data: Curate, Enrich, Associate and map to MITRE ATT&CK framework with help of Machine Learning Engine	10	Select	0	
	FUNCTIONAL - ANALYTICS				
17	The solution should be able to present a clear single screen that outlines all known information around an atomic IOC, including confidence score, tags, sources, referring URLs, referring threat bulletins, threat actors, other tracking parties, ongoing analyses, campaigns, and other IOCs.	10	Select	0	
18	The solution should support link analysis using network graphs or similar, such than an analyst can pivot iteratively from an IOC to understand related intelligence	10	Select	0	
19	The solution should allow the linking of any indicator to strategic data such as threat actor or campaign data.	10	Select	0	
20	Run enrichment tools on an IOC to gain further context. The client should create user accounts on the Enrichment Sources and activate them.	10	Select	0	
21	The solution should support the Killchain, Mitre ATT&CK and STIX model.	10	Select	0	
22	The solution should support mapping security controls against Mitre ATT&CK.	10	Select	0	
23	The solution should enable Rapid Detection and Response of Matches within the environment to threat adversaries and indicators.	10	Select	0	

Threat Inteligence Platform (TIP)					
S.No	Required Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
24	The solution should enable strategic matching leading to find associated indicators that have impacted the environment. The detection should be retrospective and allows the analyst to search back in seconds without going back to the SIEM solution or any other tool. The retention is bounded to the POV period.	10	Select	0	
25	The solution should be able to scan web rendered pages and pdfs to detect threats and bring back information to the analyst's fingertips.	10	Select	0	
26	The solution should be able to create a report or investigation using threats identified and content from web rendered pages and pdfs.	10	Select	0	
27	The solution should use the Natural Language Processing to find IOCs and TTPs on the webpage or the PDF file.	10	Select	0	
28	The NLP tool or equivalent should map the attack information on the document or the webpage to the relevant MITRE ATT&CK TTP.	10	Select	0	
29	The solution should be able to answer questions related to Threat Intelligence using closed-circuit AI. And it shouldn't search the web for answers.	10	Select	0	
	FUNCTIONAL - EXPORT				
30	The solution should support export of IOCs to CSV, STIX	10	Select	0	
31	The solution should support the rendering of any threat bulletin or any other threat intelligence product created by the platform to human-readable PDF	10	Select	0	
	FUNCTIONAL - COLLABORATION				
32	The solution should be capable of not sharing any data externally unless explicitly marked.	10	Select	0	
33	The solution should be able to share data publicly or privately.	10	Select	0	
34	The solution should support the ability of multiple analysts in the organisation to work collaboratively on the same ticket or case, such as editing or adding text, comments, IOCs, and threat entities	10	Select	0	
	FUNCTIONAL - INTEGRATION AND SUPPORT				
35	The solution should include applications to integrate and automatically manage a data feed from the solution to the security systems that the organisation requires to use threat intelligence from the system. For POV purposes we will integrate with the SIEM solution.	10	Select	0	
36	The solution should permit user-definable filters such as for a minimum confidence score to determine which new intelligence is synchronized to the downstream security system	10	Select	0	
37	The solution should permit indicators to be synchronized to a downstream system based on tags applied to the indicator, such as might result from an analyst tagging an indicator to be actioned by a security system	10	Select	0	
TOTAL MARKS		550		0	

NOTE: Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or " Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product

Primary Storage

In case the model (storage/size/any other spec) is different for different environments, compliance is to be provided for each make/model separately

Make of the Storage				
Model of the Storage				
S.No.	**Minimum Technical Specification**	**Updated in Addendum**	**Vendor Compliance (Yes/No)**	**Reference Page Number/Clause Number in Bidder's Technical documents**
1	The proposed array should be an all-NVMe array with active-active multi-controller/node scale-out architecture. The array should be scalable to at-least 4 active-active storage controllers/nodes, Proposed Storage should suppport non-disruptively upgrades, and proposed storage should support single/Dual drive capacity upgrade.The proposed array should support data in place upgrade to higher models of the same storage family.	The RFP Requirement is applicable		
2	The proposed array should have multi-controller architecture with support of NVMe media for optimal storage performance.	The RFP Requirement is applicable		
3	The proposed array should be an unified storage which support both SAN & NAS	The RFP Requirement is applicable		
4	The proposed array should be configured using all NVMe drives on Industry standard RAID6 and should be able to deliver at least 1,50,000 IOPS (8K block size, 80% Read/20% Write) with minimal latency for both read & write IOs. Mentioned performance numbers should be achieved with data reduction techniques like Compression & deduplication and data Encryption turned ON. OEM should submit the document / official sizing tool output stating the above-mentioned performance metrics capability of the proposed system. These performance numbers should be delivered after considering the overheads of deduplication, compression and encryption. The capacity to be configured as a single/multiple storage pool which should be accessible to both the controllers simultaneously for Read & Write operations.	The proposed array should be configured using all NVMe drives on Industry standard RAID6 and should be able to deliver at least 1,00,000 IOPS (8K block size, 80% Read/20% Write) with minimal latency for both read & write IOs. Mentioned performance numbers should be achieved with data reduction techniques like Compression & deduplication and data Encryption turned ON. OEM should submit the document / official sizing tool output stating the above-mentioned performance metrics capability of the proposed system. These performance numbers should be delivered after considering the overheads of deduplication, compression and encryption. The capacity to be configured as a single/multiple storage pool which should be accessible to both the controllers simultaneously for Read & Write operations.		
5	Proposed storage solution should be offerred with minimum 2 controllers with minimum 256 GB DRAM Cache memory on the entire storage Solution. The solution should scale to atleast 512GB Cache memory by adding additional controller. The proposed array must protect data in cache during a manual power down or an unexpected power outage by vaulting to flash storage. The NVMe SSD capacity drives must not be used for any caching requirements of the storage. The caching requirements of storage must be factored separately	Proposed storage solution should be offered with minimum 2 controllers with minimum 256GB DRAM Cache memory on the entire storage Solution. The solution should scale to at least 512 GB Cache memory by adding additional controller. The proposed array must protect data in cache during a manual power down or an unexpected power outage by vaulting to flash storage. The caching requirements of storage must be factored separately		
6	The proposed array should be designed with full redundancy across all components at both the hardware and software level enabling the system to have 99.9999% availability or more	The RFP Requirement is applicable		
7	The proposed array should support FC, iSCSI , (NFS v4.0 or above)/ (SMB 3.1 or above), NVMe/TCP, NVMe/FC from day one.	The RFP Requirement is applicable		
8	The proposed array should be configured with at least 8 x 32Gbps & 8 x 10Gbps optical front-end ports & Proposed storage should support 100GbE backend.	The proposed array should be configured with at least 8 × 32Gbps & 8 × 10/25Gbps optical front-end ports and should support 100GbE connectivity for host/backend connectivity.		
9	The storage must be configured with proposed storage usable capacity after dedupe and compression. It should be scalable to at-least 2x usable flash NVMe capacity on the same storage Array. The storage should support volume movement within the cluster. Addition of controllers/nodes in the same cluster should not cause any downtime and the system should automatically detect and add new controllers/nodes to the cluster.	The RFP Requirement is applicable		
10	The proposed array must support the latest industry standard (No proprietary) dual ported NVMe TLC / QLC drives.	The RFP Requirement is applicable		
11	The proposed array should support enterprise class data services including - Thin Provisioning, Inline Compression & Deduplication, replication. Data reduction must be supported on block and vVol. The data reduction feature should have no performance impact on the storage due to DRR.	The RFP Requirement is applicable		
12	Proposed storage array should support major Operating systems including Windows 2019, 2022, 2025 RedHat, SUSE, Ubuntu, Oracle, VMWare etc.	The RFP Requirement is applicable		

S.No.	Minimum Technical Specification	Updated in Addendum	Vendor Compliance (Yes/No)	Reference Page Number/Clause Number in Bidder's Technical documents
13	The proposed array must have capability to create snapshots in the proposed storage array for block, Proposed storage solution should support snapshot creation using ROW/WORM algorithm. Storage arrays should have ability to use snapshot as writable volume. These snapshots should be secure and immutable.	The RFP Requirement is applicable		
14	Proposed array should include LUN level priority based QoS engine which is easy to manage. Proposed solution should also have functionality so that a volume with a high-performance policy can be configured handle more IOPS than a volume with a medium-performance policy.	The RFP Requirement is applicable		
15	The proposed array should be proposed with native IP ports for remote replication to DR site with appropriate licenses. If separate FCIP routers are required for replication, then the same should be included in the BOM (Min 2 Nos per site).Proposed storage system should be capable of native storage based asynchronous replication .	The RFP Requirement is applicable		
16	The proposed array should be supplied with native Storage management software with Web based GUI capable of generating customized reports, real time monitoring, at least 1 year of historical performance data for analysis and trending, capacity utilization monitoring.	The RFP Requirement is applicable		
17	The proposed Storage solution should support or integrate with software (either OEMprovided or third-party) capable of automating and orchestrating application/database-consistent copies for applications including, but not limited to, MSSQL, Oracle, Exchange, to support use cases such as data repurposing, off-host backup, Test/Dev, Reporting, etc.	The RFP Requirement is applicable		
18	Proposed storage solution should support below integration options to enable DevOps and Infrastructure automation. All mentioned options should be officially supported by storage OEM. a) Support for REST API b) Support for Kubernetes Persistent Volumes using Container Storage Integration (CSI) c) Support for Ansible d) Support for PowerShell modules	The RFP Requirement is applicable		
19	The proposed array must include SED (or hardware) based data at rest encryption solution to encrypt data on all drives (AES 256 bit) with embedded automated key management. Encryption should seamlessly work with all the storage features and without any performance penalty.	The RFP Requirement is applicable		
20	Bank will not return the defective disk(s) in case of disk failure	The RFP Requirement is applicable		
21	If the OEM proposes effective storage capacity, then DRR should be applicable for the entire contract period. Incase, the DRR is not achieved anytime during the contract period, the OEM is liable to supply the additional drives/capacity to meet the required performance and effective capacity at no additional cost to the bank.	The RFP Requirement is applicable		
22	The proposed storage model should not be end of sale product at the time of bid submission, and supportability (End of Life or End of support) of the product should be available for the entire contract period. Bidder to submit the undertaking on OEM's letterhead as per Annexure 26: Undertaking – Support & Launch Confirmation.	The RFP Requirement is applicable		
	EXPERIENCE			
23	The proposed make of the storage should have been implemented in at least 2 scheduled commercial bank with 1500 branches for security solutions/Core banking system/ Datawarehouse/Datalake/Other critical system of the bank like treasury/NEFT RTGS/BFSI	The RFP Requirement is applicable		

NOTE	It is to be noted that the OEM shall submit a compliance statement confirming 100% compliance with all the above technical requirements of the RFP. The compliance statement shall be submitted for each and every model of the proposed primary storage offered as part of the solution.

x86 Servers

In case the model (Server/processor/memory/HDD/any other spec) is different for different application/deployment zone/environments, compliance is to be provided for each make/model separately

Make of the server				
Model of the server				
S.No.	**Item**	**Minimum Technical Specification**	**Vendor Compliance (Yes/No)**	**Reference Page Number/Clause Number in Bidder's Technical documents**
1	Processors	Latest upto 64 cores dual processor model (Intel Xeon or AMD EPYC) with base clock speed of 2.2 GHz or better as per the requirement and proposition proposed by the bidder		
2	Chipset	Processor OEM Chipset compatible with the offered processors.		
3	Internal Storage	The server should Support minimum 8 hot-swappable NVMe drives or more		
4		Server should be supplied with 2x 1.92TB NVMe SSD or higher. Bank will not return the defective disk(s) in case of disk failure		
5		The Server hardware RAID controller should support the following configurations RAID 0, 1, 5, 6, 10, 50, and 60. The raid controller should have minimum 4GB NV cache or higher		
6	Memory	Should be configured with 1TB memory or more Should have minimum 24 number of DIMM slots per server and support 6400MT/s or higher Dual Rank DDR5 memory or higher		
7	Operating System	Must be supplied with enterprise-level OEM supported Operating System and Virtualization solution, as required		
8	Network	2x Dual Port card with 25G SFP+ Ports with optics		
9	SAN Connectivity	2 x Dual Port 32 Gbps FC Card		
10	PCIe Slots	Should have minimum 4 or more PCIe Generation 5.0 slots or higher		
11		Should have a cyber-resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks		
12		Should provide effective protection, reliable detection & rapid recovery using:		
13		Silicon-based Immutable Hardware Root of Trust		
14		Signed cryptographic firmware updates		
15		Dynamic USB Port Management		
16		Secure default passwords		

S.No.	Item	Minimum Technical Specification	Vendor Compliance (Yes/No)	Reference Page Number/Clause Number in Bidder's Technical documents
17	Security	Shall provide dynamic system lock down server to prevent malicious attacks against embedded firmware and configuration drift in your datacenter without need to reboot the server.		
18		Persistent event logging including user activity		
19		Secure alerting		
20		Should be able to verify BIOS integrity and authenticity from malicious firmware and support automatic BIOS recovery if BIOS is corrupted (either due to a malicious attack, or due to a power loss during the update process, or due to any other unforeseen event).		
21		Shall support boot from SAN and Rapid OS Recovery In the event of a corrupted OS image		
22		Support Secure System Erase to erase sensitive data and settings from the server storage devices and server non-volatile stores such as caches and logs so that no confidential information unintentionally leaks		
23		Configuration upgrades should be only with cryptographically signed firmware and software		
24		Should provide system lockdown feature to prevent change (or "drift") in system firmware image(s) & prevent malicious modification of server firmware		
25		Intrusion alert in case chassis cover being opened		
26	Management	Real-time power meter, temperature monitoring, customized exhaust temperature and System Airflow Consumption		
27		Silicon root of trust, authenticated BIOS, signed firmware updates and BIOS Live Scanning for malicious firmware		
28		Telemetry Streaming		
29		Idle Server Detection		
30		Power control, Boot control		
31		The management software should collect system information (including impending component failure) from the device that generated the alert and should be able to send the information securely to OEM to Support to troubleshoot the issue and provide an appropriate solution.		

S.No.	Item	Minimum Technical Specification	Vendor Compliance (Yes/No)	Reference Page Number/Clause Number in Bidder's Technical documents
32		OEM's management software should be provided		
33		Firmware and configuration baselines for compliance monitoring and enable automated updates on schedule.		
34		Scope based access control to limit Users to specific group of devices		
35		Bare-metal server deployment and cloning		
36		Should have the following ports for server connectivity		
37	Ports	● 3 USB 2.0 ports or higher		
38		● 1 VGA port		
39		Supports hot swappable redundant fans		
40	Others	Supports hot swappable redundant power supplies		
41		Sliding Rail Kit to be provided along with the server		
	EXPERIENCE			
42		The proposed server make should have been successfully implemented in at least two BFSI clients, each with a minimum of 1,500 branches or offices		

SAN Switch

In case the model (Switch/Port Count/Port speed) is different for different environments, compliance is to be provided for each make/model separately

Make of the SAN Switch				
Model of the SAN Switch				
S.No.	**Minimum Technical Specification**	**Vendor Compliance (Yes/No)**	**Reference Page Number/Clause Number in Bidder's Technical documents**	**Vendor's Remarks**
1	The switch should have non-blocking architecture with all ports active with 32 G SFP+ modules , switch should also support 64G transceiver for future ugrades.			
2	The switch should be configured with base 24 port (minimum) and can be upgraded to 48 ports with port-on - demand licenses activiation			
3	The switch should support auto-sensing 64,32,16, 8 Gbit/sec FC capabilities.			
4	The switch shall support different port types such as D_Port (ClearLink Diagnostic Port), E_Port, EX_Port, F_Port, optional port-type control Brocade Access Gateway mode: F_Port and NPIV-enabled N_Port			
5	The switch must provide a maximum Aggregate bandwidth of 4Tbps (data rate) end to end or more			
6	Non disruptive Microcode/ firmware Upgrades and hot code activation.			
7	The Switch must provide autonomous Congestion control mechanisms without user intervention			
8	The Swith must be able to automatically quarantine and unquarantine slow-devices			
9	The Switch must provide Virtual Machine (VMID) support for end-to-end SAN telemetry			
10	The switch should support Frame-based trunking with up to eight SFP+ ports per ISL trunk; up to 512Gb/s per ISL trunk			
11	The Switch must support POST and online/offline diagnostics, including RAStrace logging, environmental monitoring, non-disruptive daemon restart, FCping andPathinfo (FC traceroute), port mirroring (SPAN port).			
12	The Switch must support web based management and also support CLI.			
13	The switch must support 24K frame buffers			
14	The Switch must support SAN Analytics with parallel SCSI and NVMe-FC analytics			
15	Should provide redundant and hot pluggable components.			
16	The switch should support Front to back and back to Front airflow			
17	The switch should be 1U form factor and rack mountable in a standard Rack			
	EXPERIENCE			
18	The proposed make of the SAN Switch should have been implemented in at least 2 scheduled commercial bank with 1500 branches for security solutions/Core banking system/ Datawarehouse/Datalake/Other critical system of the bank like treasury/NEFT RTGS/BFSI			

Backup Solution
In case the model (Switch/Port Count/Port speed) is different for different environments, compliance is to be provided for each make/model separately

Make of the Backup solution					
Model of the Backup solution					
S.No.	**Minimum Technical Specification**	**Updated in Addendum**	**Vendor Compliance (Yes/No)**	**Reference Page Number/Clause Number in Bidder's Technical documents**	**Remarks**
1	Proposed backup software must support backup, recovery, Long term archival and restoration from single GUI / console/unified management.	The RFP Requirement is applicable			
2	The backup soolution must provide MFA integration to ensure additional security measure against compromise for local admin and AD users.	The RFP Requirement is applicable			
3	The proposed backup solution must support efficient, source-side deduplicated data movement. The backup master servers and the media servers must be provided in high availability configuration ensuring no single point of failure.	The RFP Requirement is applicable			
4	The data protection platform must provide online, application-consistent protection for databases (Oracle, SAP HANA, Microsoft SQL Server, MongoDB, etc.) using native or online agents to enable fast, granular restores across a broad range of supported Windows, Linux, and Unix OS. It should also deliver image-level protection for virtualized environments including VMware, Microsoft Hyper-V, Nutanix AHV, OpenShift, and additionally offer Kubernetes backup and recovery – all managed through a single, unified UI console.	The RFP Requirement is applicable			
5	Proposed backup software must support Multi-Tenancy feature.	The RFP Requirement is applicable			
6	Should be able to integrate with native backup interfaces of Hyper Converged Solutions in future agentless and/or image level backup of VMs	The RFP Requirement is applicable			
7	Should be able to archive ALL workloads (VMs, DBs, Files) backup data by moving it to another disk target with different hardware using NFS/S3 protocols for long term retention and all the licenses for backup software and backup storage must be provided on day 1.	Should be able to archive ALL workloads (VMs, DBs, Files) backup data by moving it to another disk target with different hardware using NFS/S3 or equivalent industry-standard protocols for long-term retention, and all licenses for backup software and backup storage must be provided on Day 1.			
8	The proposed backup solution must support provide Data protection, Replication, Encryption, Immutability, MFA (Multi-factor authentication) and archival to external NFS/S3 based storage from day 1 and all these licenses must be included.	The proposed backup solution must support Data Protection, Replication, Encryption, Immutability, MFA (Multi-Factor Authentication) and archival to external NFS/S3 or equivalent industry-standard storage from Day 1, and all required licenses for these functionalities must be included.			

S.No.	Minimum Technical Specification	Updated in Addendum	Vendor Compliance (Yes/No)	Reference Page Number/Clause Number in Bidder's Technical documents	Remarks
9	The Proposed solution should ensure Data Protection & Archival: a) Backup and Recovery: Protects data by creating secure backups and enables fast recovery in case of failures or cyber incidents. b) Data Immutability & Encryption: Ensures that sensitive data is protected both in transit and at rest using strong encryption methods. (Backup software managed but applies on Backup Storage - WORM capability). The proposed solution and its backup appliance must provide immutable backup storage via WORM (Write Once, Read Many) or a retention-lock capability. Immutability must be backup-software-aware and integrated with the storage layer through a secure protocol and/or native API. It must be enforced automatically at the policy level — not manually configured — and propagated down to storage. The backup software and storage must operate as a single integrated system, not in silos. c) Data Integrity and Availability: Ensures that data remains intact and available for recovery in case of an outage, system failure, or cyberattack. d) Archival: Reduces the cost of storing inactive or less frequently accessed data. e) Compliance and Legal Hold: Ensures that data is retained for the necessary period as required by regulatory bodies and the organization's internal policies. f) Search and Retrieval: Enables fast and efficient retrieval of archived data, ensuring that critical information can be accessed quickly when needed. g) Long Term Retention/Forever Retention: Covers a "No Loss of Data" policy using long-term retention. h) The proposed solution should have the ability to protect all mount paths associated with disk libraries configured from a Backup/Media Server against ransomware attacks, or provide equivalent ransomware protection for backup architectures that do not use conventional mount paths or Backup/Media Servers.	The RFP Requirement is applicable			
10	The proposed backup software must be deployed in a high-availability (HA) configuration, encompassing all critical components — including media/proxy servers and the master/control server — to eliminate any single point of failure across the backup core infrastructure.	The RFP Requirement is applicable			
11	The Backup software must be able to compress and encrypt data and should also suport de-duplication.	The RFP Requirement is applicable			
12	Proposed backup solution should support archiving the long term retention copies of ALL the workloads like VMs, DB, Files, etc on *Long term Storage* using NFS/S3 protocols and required software licenses must be provided on day 1.	The RFP Requirement is applicable			
13	Solution should provide historic backup & retrieval reports for success & failure Daily, Monthly & Quarterly or as per Bank requirement.	The RFP Requirement is applicable			
14	The backup software should provide centralized management / Single interface for management of all backup and archival across applications and workloads deployed in on-premises and cloud environments	The RFP Requirement is applicable			

S.No.	Minimum Technical Specification	Updated in Addendum	Vendor Compliance (Yes/No)	Reference Page Number/Clause Number in Bidder's Technical documents	Remarks
15	The following backup and retention policy to ensure data protection, recoverability, and compliance with long-term retention needs is complied: • Daily Incremental Backup – retained for 2 weeks in disk-based appliance/backup storage • Weekly Full Backup for all data types – Retained for 4 weeks in disk-based appliance/backup storage • Monthly Full Backups – Retained for 2 Months in the same appliance/backup storage *After the 2-month period, Monthly Full backups must be migrated to long-term backup storage, where they shall be retained for the entire duration of the contract. Backup Appliance / Backup Storage Requirements * Online Backup Storage/Appliance must retain backups for a minimum period of 2 months, with each Monthly backup being preserved during this duration. * All monthly backups taken during the contract period must also be stored on long-term storage for the entire duration of the contract. *All the data, logs, information & others must be backed up using the proposed backup and retrieval solution, in accordance with the defined backup policy and retention requirements. *Regularly test and verify the integrity of backed-up data and information by performing retrieval exercises. This process should be completed prior to overwriting or replacing any previously taken backups, to ensure that the data is recoverable, intact, and usable when required.	The RFP Requirement is applicable			
16	The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data over a secure, API-based disk-to-disk (D2D) connection.	The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data using standard data protocols such as FC, iSCSI, NFS, S3.			
17	Proposed backup solution must support software based de-duplication and shall be capable of taking backup of data and workloads (irrespective of the underlying storage OEM) and the solution shall support deduplicated backup copies for long-term retention. Based on policy backup software should be able to move deduplicated backup copy to a Long term storage automatically. The proposed backup solution shall support deduplicated backup targets across leading OEM storage systems and shall not be restricted on any specific OEM/vendor.	The RFP Requirement is applicable			

S.No.	Minimum Technical Specification	Updated in Addendum	Vendor Compliance (Yes/No)	Reference Page Number/Clause Number in Bidder's Technical documents	Remarks
18	Proposed Disk Based Appliance/backup storage should have the capability to tier backup data to an external cloud storage (on premise / public cloud) and the required licenses must be provided on day 1. Proposed backup solution with storage/appliance should have redundant components (Backup Storage - controllers, Power , fans etc. and Backup Appliance - Power , fans etc.) , HA mechanism in place to avoid Single Point of Failure and should have minimum of 4x16/32 GB FC ports & 2x32G ports on each controller for Host connectivity. Proposed Backup Solution should have minimum 4x scalability of the current quoted capacity for future growth.	Proposed Disk Based Appliance/Backup Storage should have the capability to tier backup data to external storage (on-premise) and all licenses required for the proposed functionality shall be provided from Day 1. The proposed backup solution, including storage/ appliance components, shall incorporate appropriate redundancy for critical components such as controllers, power supplies, fans, etc., and shall provide an appropriate High Availability (HA) mechanism to minimize or eliminate Single Points of Failure. The proposed storage/appliance should have minimum of 4x32 GB FC ports and/or 4x10/25 GbE network ports on each controller for Host connectivity, as applicable to the proposed architecture. Proposed Backup Solution should have a scalable architecture capable of supporting minimum 4x expansion of the current quoted usable capacity for future growth, through expansion of the existing solution and/or addition of compatible components, without requiring replacement of the complete solution			
19	Proposed Disk Based backup appliance should have the ability to perform different backup, restore, replication jobs simultaneously and must support communications and data transfers through 10/25 Gb ethernet LAN over SFP+. The proposed backup appliance should be offered with minimum 4 x 10/25 Gbps NIC SFP+ or Proposed Disk Based backup storage should have the ability to perform different backup, restore, replication jobs simultaneously and Must supports communications and data transfers through 32 GB SAN, 10 Gb & 1 Gb ethernet LAN over copper and SFP+. The Proposed Backup Storage should have should have minimum of 4x16/32 GB FC ports & 2x32G ports on each controller for Host connectivity.	The RFP Requirement is applicable			
20	The proposed appliance/backup storage must ensure that all scheduled backups complete within an 8-hour backup window, with data protected via RAID 6 (or equivalent - providing 2 disk failure protection). Backup solution must support required technology and storage capacity to manage and compensate duplication across multiple pools, ensuring consistent performance and efficiency. Overheads in terms of memory, capacity, technology and IOPS to handle the bottleneck due to multiple deduplication pools should be factored and required documentation from the OEM is to be submitted along with the proposal.	The RFP Requirement is applicable			
21	Proposed Appliance/Backup Storage should support different retentions for primary and DR backup storage and should support instant copy creation on remote site for better DR readiness with support for transmitting only deduplicated unique data in encrypted format to remote sites.	The RFP Requirement is applicable			
22	The proposed backup Solution must support immutability, retention lock or equivalent feature which ensures that no data is deleted accidently.	The RFP Requirement is applicable			
23	Proposed Appliance/Backup Storage should support bi-directional, many-to-one, one-to-many, and one-to-one replication.	The RFP Requirement is applicable			
24	Proposed Appliance/Backup Storage should support 256 bit AES encryption for data at rest and data-in-flight during replication. It should offer internal and external key management for encryption.	The RFP Requirement is applicable			
25	The Proposed Appliance/Backup Storage must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism	The Proposed Appliance/Backup Storage/backup solution must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism.			

S.No.	Minimum Technical Specification	Updated in Addendum	Vendor Compliance (Yes/No)	Reference Page Number/Clause Number in Bidder's Technical documents	Remarks
26	All file system data and Metadata must be verified continuously even if parts of the file system are never accessed for reads (Automated Data Scrubbing Process)	The RFP Requirement is applicable			
27	Any modification or new data must not modify existing data blocks to prevent possibility of corruption. Any new or modified content must be written to new blocks	The RFP Requirement is applicable			
28	The appliance/storage should be configured with all the licenses backup and replication necessary for the sought functionalities.	The RFP Requirement is applicable			
29	The proposed solution shall ensure that backup expiry/immutability cannot be bypassed by any internal or external change to system time, whether by restricting time changes or by an immutability mechanism that is independent of the system clock.	The RFP Requirement is applicable			
30	Proposed Appliance/Backup Storage must offer with feasibility to protect data from accidental deletion	The RFP Requirement is applicable			
31	Regular Maintenance activities like Systems Housekeeping/Garbage Cleaning etc should be able to happen simultaneously along with regular backup and restore operations without having the need for a dedicated window	The RFP Requirement is applicable			
32	Proposed backup appliance/storage should be offered with Multi-Tenancy features which provides a separate logical space for each tenant user.	The RFP Requirement is applicable			
33	The solution should provide data validation features to ensure data integrity by validating data integrity during backup, when data is at rest and during data copy operations.	The RFP Requirement is applicable			
34	Backup is to be performed at both DC and DR. The Proposed solution must have Disk to Disk to Long term Storage (D-D-LTS) Backup solution with backup data to be kept on disk for easy retrieval.	The RFP Requirement is applicable			
35	Backup & retrieval software, Backup Appliance or Integrated applaince is to be proposed at both DC & DR with all requisite licenses for both the sites separately.	The RFP Requirement is applicable			
36	Product should offered with 24x7- 5 years (Contract period, whichever is later) onsite warranty support.	The RFP Requirement is applicable			
37	Backup software should be able to replicate backed up data in de-duplicated format (for bandwidth optimization) to another site for compliance purposes, without the need of external replication tools. All necessary licenses for achieving consistent replication of backup data should be quoted.	The RFP Requirement is applicable			
38	The proposed backup software must have the capability to integrate with snapshot based backup for data residing on popular storage devices from NetApp / Dell-EMC / Pure etc.	The RFP Requirement is applicable			
39	Backup storage/Appliance capacity expansion - whether by adding disks, adding an enclosure, or adding scale-out nodes - must be non-disruptive, and no additional storage-side licence shall be required to consume the expanded capacity where the backup software"s protected-capacity licence already covers the data being protected.'	The RFP Requirement is applicable			
40	The proposed solution should provide the High Availability with failover/failback capabilities for the Backup Management server without the need of clustering at OS level and any additional license requirements.	The RFP Requirement is applicable			
41	Comprehensive reporting of media, backup server, jobs, analytics should be offered as part of the functionality in the supplied software either natively or through additional reporting software.	The RFP Requirement is applicable			
42	The proposed storage model should not be end of sale product at the time of bid submission, and supportability (End of Life or End of support) of the product should be available for the entire contract period. Bidder to submit the undertaking on OEM's letterhead as per Annexure 26: Undertaking – Support & Launch Confirmation.	The RFP Requirement is applicable			

S.No.	Minimum Technical Specification	Updated in Addendum	Vendor Compliance (Yes/No)	Reference Page Number/Clause Number in Bidder's Technical documents	Remarks
	EXPERIENCE				
43	The proposed make and category of the backup solution & appliance should have been implemented in at least 2 scheduled commercial bank with 1500 branches.	The RFP Requirement is applicable			

NOTE It is to be noted that the OEM shall submit a compliance statement confirming 100% compliance with all the above technical requirements of the RFP. The compliance statement shall be submitted for each and every model of the proposed Backup Solution and

Long Term Storage

In case the model is different for different environments, compliance is to be provided for each make/model separately

Make of the Long Term Storage					
Model of Long Term Storage					
S.No.	**Minimum Technical Specification**	**Updated in Addendum**	**Vendor Compliance (Yes/No)**	**Reference Page Number/Clause Number in Bidder's Technical documents**	**Remarks**
1	Proposed storage would be proposed for long retention of Backup data (Protocol- NAS/CIFS/SMB/S3/SAN storage (Protocol- iSCSI)	Proposed storage would be proposed for long retention of Backup data (Protocol- NAS/CIFS/SMB/S3/SAN storage (Protocol- iSCSI/SAN)			
2	Bank is looking for Long term storage for the duration of the Contract. Bidder to design and propose the solution for storing the backups for the druation of the contract with adequate interfaces for perofmring the backup & retrieval within the defined period and as per the terms of the RFP. Interface should be design to ensure that Data / logs/Informations are in the proposed storage after the duration mentioned in the RFP. The Backed up data / logs need to be restored in the respective technology for forensic and other requriement of the bank etc.	The RFP Requirement is applicable			
3	Bank is looking for Long term storage for the duration of the Contract. Bidder to design and propose the solution for storing the backups for the druation of the contract with adequate RAID. Proposed Sizing should be proposed on RAID 6	The RFP Requirement is applicable			
4	• Bidder is required to propose the long-term backup storage at both the Data Centre (DC) and Disaster Recovery (DR) sites and must adequately sized the storage to retain backup data for the entire duration of the contract. • The sizing should account for data growth, retention policies, and restore requirements, ensuring reliable and compliant backup management throughout the contract period.	The RFP Requirement is applicable			
5	The proposed storage model should not be end of sale product at the time of bid submission, and supportability (End of Life or End of support) of the product should be available for the entire contract period. Bidder to submit the undertaking on OEM's letterhead as per Annexure 26: Undertaking – Support & Launch Confirmation.	The RFP Requirement is applicable			
	EXPERIENCE				
6	The proposed make and category of the storage should have been implemented in at least 2 scheduled commercial bank with 1500 branches	The RFP Requirement is applicable			

NOTE	It is to be noted that the OEM shall submit a compliance statement confirming 100% compliance with all the above technical requirements of the RFP. The compliance statement shall be submitted for each and every model of the proposed Long Term

Load Balancer

In case the model is different for different environments, compliance is to be provided for each make/model separately

Make of the Load Balancer			
Model of the Load Balancer			

S.No.	Minimum Technical Specification	Compliance (Yes/No)	Reference Page Number/Clause Number in Bidder's Technical documents	Remarks
1	The proposed solution should be a dedicated appliance as ADC not as add on license Feature on NGFW and WAF.			
2	The Appliance should have dedicated 1x1GbE port for management and 4x10GbE SFP+ p orts and multicore CPU, minimum 4 TB HDD and dual power supply.			
3	The SLB OEM should support 7K SSL TPS for RSA 2K key, 10K SSL TPS for ECDSA P25			
4	The appliance should have dedicated SSL Acceleration hardware card for handling SSL Traffic. The SSL traffic should not be process by CPU of the appliance			
5	The solution should able to load balancer both TCP and UDP based applications with layer 2 to layer 7 load balancing including WebSocket and WebSocket Secure.			
6	The solution should support server load balancing algorithms i.e. round robin, weighted round robin, least connection, Persistent IP, Hash IP, Hash Cookie or equivalent, shortest response, proximity, SNMP, SIP session ID etc.			
7	The solution should support Multi-level virtual service policy routing ,-Static, default and backup policies for intelligent traffic distribution to backend servers			
8	The solution should support for policy nesting at layer 7 and layer 4. it should able to combine layer4 and layer7 policies to address the complex application integration.			
9	The solution should have script based functions support for content inspection, traffic matching and monitoring of HTTP, SOAP, XML, diameter, generic TCP, TCPS. It should support ePolicies or equivalent to customize new features/rules to re-direct the traffic on specific parameters.			
10	The solution using e-policy or equivalent then should support algorithms including round robin, least connections, shortest response, persistence ip, hash ip, hash ip and port, consistent hash IP and snmp			
11	The solution should provide application & server health checks for well-known protocols such as ARP, ICMP, TCP, DNS, RADIUS, HTTP/HTTPS, RTSP etc.			
12	The Solution should provide real time Dynamic Web Content Compression to reduce server load and solution should provide selective compression for Text, HTML, XML, DOC, Java Scripts, CSS, PDF, PPT, and XLS Mime types.			
13	The solution should provide advanced high performance memory/packet based reverse proxy Web cache; fully compliant with HTTP1.1 to enhance the speed and performance of web servers			

S.No.	Minimum Technical Specification	Compliance (Yes/No)	Reference Page Number/Clause Number in Bidder's Technical documents	Remarks
14	The solution should provide support for cache rules/filters to define granular cache policies based on cache-control headers, host name, file type, max object size, TTL objects etc..			
15	The proposed load balancing solution should support a license upgrade mechanism that allows for the enablement of additional features on the same physical or virtual appliance, without requiring hardware replacement. Where applicable, the solution should be capable of integrating with or supporting secure machine-based authentication mechanisms for access to corporate resources.			
16	The solution should provide secure online application delivery using hardware-based high performance integrated SSL acceleration hardware. SSL hardware should support both 2048,4096 bit keys for encrypted application access.			
17	The solution must support Single Sign-On (SSO) for web based applications and web based file server access. It should also supports SAML secure application access			
18	The solution should provide performance optimization using TCP connection multiplexing, TCP buffering and IEEE 802.3ad link aggregation. Support for TCP optimization options including windows scaling, timestamp & Selective Acknowledgement for enhanced TCP transmission speed TCP optimization option configuration should be defined on per virtual service basis not globally.			
19	The solution should support certificate parser and solution should integrate with client certificates to maintain end to end security and non-repudiation. It should support Certificate format as "OpenSSL/Apache, *.PEM", "MS IIS, *.PFX", and "Netscape, *.DB".			
20	The solution should support OCSP protocol to check the validity of the certificates online. Certificate bases access control, CRL's (HTTP, FTP, and LDAP) support.			
21	The solution should provide full ipv6 support and OEM should be IPv6 gold-certified. OEM should be listed vendor for ipv6 phase-2 certification.			
22	The solution should support advance ACL's to protect against network based flooding attacks. Administrator should able to define ACL's rules based on connections per second (CPS) and concurrent connections (CC), cookie value.			
23	Should support QOS for traffic prioritization, CBQ , borrow and unborrow bandwidth from queues. It should provide QOS filters based on port and protocols including TCP, UDP and ICMP Protocols. Should support rate shaping for setting user defined rate limits on critical application.			
24	The solution should support site selection feature to provide global load balancing features for disaster recovery and site redundancy.			
25	It should support advance functions Authoritative name sever, DNS proxy/DNS NAT, full DNS server with DNSEC, DNS DDOS, application load balancing from day one. It should be capable of handling complete Full DNS bind records including A,MX, AAAA, CNAME, PTR, SOA etc.			

S.No.	Minimum Technical Specification	Compliance (Yes/No)	Reference Page Number/Clause Number in Bidder's Technical documents	Remarks
26	The solution should provide comprehensive and reliable support for high availability and N+1 clustering based standard VRRP RFC 2338 or equivalent on Per VIP based Active-active & active standby unit redundancy mode.			
27	the solution should support Stateful session failover with N+1 clustering support when deployed in HA mode.			
28	The solution should support floating MAC address to avoid MAC table updates on the upstream routers/switches and to speedup the failover. It should support for secondary communication link for backup purpose			
29	The solution should support floating IP address and group for stateful failover support. It should support built in failover decision/health check conditions including, CPU overheated, system memory, process health check, unit failover, group failover and reboot			
30	The solution should also have option to define customized rules for gateway health check - the administrator should able to define a rule to inspect the status of the link between the unit and a gateway			
31	The appliance should have extensive reporting and logging with inbuilt tcpdump like tool and log collection functionality. The appliance should have SSH CLI, Direct Console, SNMP, Single Console per Cluster with inbuilt reporting.			
32	The solution should support XML-RPC for integration with 3rd party management and monitoring of the devices. The appliance should provide detailed logs and graphs for real time and time based statistics			
33	The appliance must support multiple configuration files with 2 bootable partitions for better availability and easy upgrade / fallback. The system should support led warning and system log alert for failure of any of the power and CPU issues			
34	OEM should have TAC & R&D facility in INDIA. The proposed solution should be up and running in PSU/PSE/Govt. Organization within the last 5 years			

S. No	Solution Name	Maximum Mark Allocated	Maximum Mark Obtained	Respective Solution Compliance (%)
1	TI Feed	**210**	0	0.00%
2	Red Teaming	**390**	**0**	0.00%
3	Threat Hunting	**150**	**0**	0.00%
4	ASM	**400**	**0**	0.00%
5	Breach Attack Simulation	**110**	**0**	0.00%
6	**Digital risk management**	**650**	**0**	0.00%
7	Dark Web monitoring	**630**	**0**	0.00%
8	Phishing Simulation	**720**	**0**	0.00%
GRAND TOTAL		**1260**	**0**	**0.00%**

Instructions

Maximum Marks	Compliance (S/C)	Maximum Mark
10	**S (Standard):**	This indicates that the requirement is covered by the standard product functionality. It includes features available out-of-the-box, as well as those achievable through parametrization or rules configuration.
3	**C (Customization):**	Requirements marked as C (Customization) go beyond what is available or possible through standard product configuration. Customization involves: Development of custom code Creation of new functionalities or interfaces Modifications that may impact upgrade paths or require specific deployment and testing cycles User interface enhancements or custom-built screens Creation of entirely new functionality not supported by the base product

S.No	Instruction
1	Bidder must mandatorily mention the exact page number & clause or section reference from their submitted technical proposal or OEM product documentation which demonstrate compliance with each criteria (specification). Any Response marked as compliance without a valid page reference/section reference, shall be treated as in-complete and may be liable for rejection/scoring penalties
2	Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or " Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product
3	All Regulatory guidelines requirements as on the date of Bid Submission should be complied from day 1. Bidder/OEM is also required to comply with all the guidelines (regulatory & statutory) issued during the contract period

4	In case bidder has provided the response which is neither "S" or "C". The requirement shall be considered as "No"or "N", the bid shall be liable for rejection
5	All the above mentioned features should be available form the day 1.

Threat Intelligence Feed						
S.No.	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
1	Threat Intel provider must have Intel collection in more than 20 languages broad coverage across both the Western and Eastern worlds.	RFP Clause is applicable	10	Select	0	
2	The provider should be having a technology partnership or integration with leading vendors in SIEM, and other devices to integrate the feeds.	RFP Clause is applicable	10	Select	0	
3	The TI feed should seamlessly integrate with SIEM, SOAR, and other security tools to automatically enrich and triage alerts with the most comprehensive threat data available and our unified verdict.	RFP Clause is applicable	10	Select	0	
4	The Threat Intel provider must provide browser extensions to perform lookups from within the browser for Threat Intel search. Or The Threat Intel provider must provide web interface to perform lookups for Threat Intel search.	RFP Clause is applicable	10	Select	0	
5	The proposed TI solution should be capable of representing Indicator Scores.	RFP Clause is applicable	10	Select	0	
6	Must have the capability for Web searching (reports, IoCs, IoC modifiers, etc.)	RFP Clause is applicable	10	Select	0	
7	The portal must provide IoC lookups (reputation & analysis). This capability should give insights to understand how malware files act and communicate. The TI tool should detonates files in virtual controlled environments to trace their activities and communications, producing detailed reports including opened, created and written files, created mutexes, registry keys set, contacted domains, URL lookups, etc. This execution activity should be indexed in a faceted fashion in order to allow for instantaneous lookups.	The portal must provide IoC lookups (reputation & analysis). This capability should give insights to understand how malware files act and communicate. The TI tool should detonate/analyse files in virtual controlled environments or through equivalent malware-analysis capabilities to trace their activities and communications, producing detailed reports including opened, created and written files, created mutexes, registry keys set, contacted domains, URL lookups, etc. This execution activity should be indexed in a faceted fashion in order to allow for instantaneous lookups.	10	Select	0	
8	The provider must have the Retrohunt retrospection window for threat investigavation & tracking	RFP Clause is applicable	10	Select	0	
9	The provider must have capability for (Malware) file corpus downloads via web interface for further analysis. Or The provider must have capability for (Malware) analysis while scanning through multiple engines including sandbox, attribution engine & similarity engine.	RFP Clause is applicable	10	Select	0	
10	The provider must have the capability to monitor threats beyond your perimeter covering Credential monitoring :Automatically alerts you about the presence of specific user accounts in compromised credentials data collected from the deep and dark web. Malicious domain monitoring :Looks for new domain names that mention your company or brand names, indicating fraud and brand reputation attack preparation. Data leak monitoring :Detects exposures of your sensitive information, such as financial data, trade secrets, or customer information. Underground monitoring :Detects when attackers refer to your brands, hosts, domains, and other identifiers on the deep and dark web.	RFP Clause is applicable	10	Select	0	
11	The provider must have the capability to provide external Asset discovery and monitoring (assets) which will help organisation to get an attacker's viewpoint, this should give capability to identify vulnerabilities, misconfigurations, and their potential impact on organization.	RFP Clause is applicable	10	Select	0	
12	The provider must cover Categorized threat lists for Ransomware & Malicious network infrastructure which will help to readily download and integrate actionable threat intelligence focused on specific threat types into their security tools.	RFP Clause is applicable	10	Select	0	
13	TI portal must have capability to search that allows users to ask natural language questions to get a generative AI-powered/AI-driven overview on their question	TI portal must have capability to search that allows users to obtain AI-generated summaries and insights from threat intelligence lookups, including through natural language or equivalent AI-driven capability.	10	Select	0	
14	TI provider must have capability to create YARA rules against URLs, domains and IP addresses and hunt for new network indicators that match certain metadata.	TI provider must have capability to investigate against URLs, domains and IP addresses and identify related network indicators that match certain metadata. The provider may implement this through YARA Rules or relationship graph or equivalent analytical capability.	10	Select	0	
15	Threat intelligence provider must provide the relationships graph to understands the relationship between files, URLs, domains, IP addresses and other items encountered in an ongoing investigation (threat actors, campaigns, malware families, etc.). With it, TI analyst can pivot intelligently over any of the malware artifacts in your graph and synthesize your findings into a threat map.	Threat intelligence provider must provide the relationships graph to understand the relationship between files, URLs, domains, IP addresses and other items encountered in an ongoing investigation. With it, TI analyst can pivot intelligently over any of the malware artifacts in your graph and synthesize your findings into a threat map.	10	Select	0	

Threat Intelligence Feed						
S.No.	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
16	The provider must provide the curated Strategic Reporting generated by threat intelligence analysts in the following areas: a) Industry: Reports on threats specific to an industry vertical, considering various adversary motivations. b) Region / Country profile: Reports on threats targeting a particular country or geographic region, across different adversary motivations. c) Trends & Forecasting: Analysis of threat actor tactics, trends, and types of threat activity, potentially including historical reviews and predictions. d) Executive Perspective: Analysis about cyber threats relevant to events or business circumstances, geared toward a strategic leadership audience. This report type also includes Intelligence-at-a-Glance reports, which provide a weekly snapshot into newly produced reports, blogs, webinars; as well as some insight into customer interests	The provider must provide the curated Strategic Reporting generated by threat intelligence analysts in the following areas: a) Industry: Reports on threats specific to an industry vertical, considering various adversary motivations. b) Region / Country profile: Reports on threats targeting a particular country or geographic region, across different adversary motivations. c) Trends & Forecasting: Analysis of threat actor tactics, trends, and types of threat activity, potentially including historical reviews and predictions. d) Executive Perspective: Analysis about cyber threats relevant to events or business circumstances, geared toward a strategic leadership audience. Equivalent executive summary reports covering relevant TTPs shall also be acceptable.	10	Select	0	
17	The provider must provide curated details on various aspects of adversary activities, with a focus on their methods and behaviors. Including: a) Actor Profile: In-depth look into a specific threat actor's tactics, techniques, and procedures. b) TTP Deep Dives: Detailed analysis into a threat actor and the tactics, techniques, and procedures (TTPs) they use to achieve specific goals. c) Event Coverage / Implication: Analysis on the implications of a recent event or campaign conducted by a threat actor. d) Malware Profile: Technical analysis of a representative sample of a code family. This report type typically includes file characteristics, host- and network-based indicators, configuration information, and details of code execution	The provider must provide curated details on various aspects of adversary activities, with a focus on their methods and behaviors. Including: a) Actor Profile: In-depth look into a specific threat actor's tactics, techniques, and procedures. b) TTP Deep Dives: Detailed analysis into a threat actor and the tactics, techniques, and procedures (TTPs) they use to achieve specific goals. c) Event Coverage / Implication: Analysis on the implications of a recent event or campaign conducted by a threat actor. d) Malware Profile: Technical analysis of a representative sample of a code family.	10	Select	0	
18	The TI provider must have a vulnerability intelligence module or attack surface management capability to collect technical and threat reporting, identify vulnerabilities (including those exposed on internet-facing assets), and provide stakeholders with clarity for informed decision-making, resource prioritization, and patch/mitigation/version management.	RFP Clause is applicable	10	Select	0	
19	TI portal must provide personalized Threat Landscape by creating customizable Profiles so that TI analysts can focus only on the threats that matter most to PSB	RFP Clause is applicable	10	Select	0	
20	The TI portal should have the capability to scan the files/URL's submitted on non-shareable basis ie privacy preserving. The submitted file should not be shared with anyone. The analysis should include a) Malicious flags via crowdsourced detection rules (YARA, Sigma, IDS) b) Suspicious properties via Static analysis c) Dynamic analysis in multiple sandboxes d) Malware config extraction e) Threat Intel Enrichment for IoCs (threat reputation, geolocation ITW prevalence, etc.) f) Clustering & Similarity Analysis, letting you pivot to similar objects based on multiple similarity algorithms	RFP Clause is applicable	10	Select	0	
20		The threat feeds must provide relevant threat intelligence feeds, including IP Reputation, Malicious URL, Phishing URL, Botnet C&C URL, and malicious/suspicious Domains, that must be updated at least once every 1 hour to 4 hours and every 1 week for CVEs and other relevant indicators, ensuring near real-time coverage of emerging threats.	10	Select	0	
TOTAL MARKS			210		0	

Red Teaming Services						
S.No.	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
1	Run a real-world scenario that's designed to measure how well organization's defensive and response capabilities will stand up against social, physical, network and application attacks from a simulated real-life adversary.	RFP Clause is applicable	10	Select	0	
2	Recognizing security issues within the Bank.	RFP Clause is applicable	10	Select	0	
3	Perform legal assessment on local/remote networks. Clarification: "Perform legal assessment on local/remote networks" as part of a Red Teaming exercise in India is to ensure the simulated attack remains fully compliant with stringent Indian laws, especially those concerning data privacy, data sovereignty, and authorized access to computer systems, thereby protecting the client and the Red Team from criminal or civil liability.	RFP Clause is applicable	10	Select	0	
4	Examining an organization for weaknesses as through the eyes of an industrial spy or a competitor.	RFP Clause is applicable	10	Select	0	
5	Social engineering.	RFP Clause is applicable	10	Select	0	
6	Trusted systems testing.	RFP Clause is applicable	10	Select	0	
7	Password Cracking.	RFP Clause is applicable	10	Select	0	
8	Identification of possible weak points in physical and logical security.	RFP Clause is applicable	10	Select	0	
9	Vulnerability Research and Verification (automated and manual).	RFP Clause is applicable	10	Select	0	
10	Competitive Intelligence.	RFP Clause is applicable	10	Select	0	
11	Internal application Testing.	RFP Clause is applicable	10	Select	0	
12	Exploit Research.	RFP Clause is applicable	10	Select	0	
13	Security testing of Firewalls, ACL other security devices.	RFP Clause is applicable	10	Select	0	
14	Identification of Rouge Devices.	RFP Clause is applicable	10	Select	0	
15	Cyber war game. "Cyber war game" in the context of Continuous Automated Red Teaming (CART) refers to a highfidelity, strategic simulation of a major cyber incident designed to test not just technology, but also the organization's people, processes, and leadership decision-making. While CART's automated attacks constantly test technical defenses (the "if" and "how" of a breach), the "Cyber war game" component focuses on the strategic, non-technical response to a catastrophic event.	RFP Clause is applicable	10	Select	0	
16	Determining appropriate countermeasures to thwart malicious hacking.	RFP Clause is applicable	10	Select	0	
17	Conduct simulated cyber-attacks on the bank's infrastructure.	RFP Clause is applicable	10	Select	0	
18	Validate protections and monitoring around high-value systems.	RFP Clause is applicable	10	Select	0	
19	Blended, covert test that can encompass network testing, phishing, wireless, and physical attacks. "Blended, covert test that can encompass network testing, phishing, wireless, and physical attacks" as part of a Red Teaming program (or Continuous Automated Red Teaming - CART) is to conduct a realistic, end-to-end, multi-vector attack simulation that replicates the methods of a sophisticated, determined adversary. This type of test is essential for validating an organization's overall security posture across all three pillars: People, Process, and Technology.	RFP Clause is applicable	10	Select	0	
20	The solution should perform active attacks on bank's systems with pre-specified goals and identify the possible attack paths and risks through objective based red teaming attacks.	RFP Clause is applicable	10	Select	0	
21	The solution should launch multi-stage attacks, which includes network attacks and application attacks on the discovered digital attack surface to identify breach and attack paths.	RFP Clause is applicable	10	Select	0	
22	The solution should continuously discover the attack paths that lead to critical assets, enabling full visibility into bank's security posture.	RFP Clause is applicable	10	Select	0	
23	The solution should provide security control validation where bank can assess the effectiveness of the existing controls and determine whether they are exposed.	RFP Clause is applicable	10	Select	0	
24	The solution should continuously challenge, assess, and optimize your security controls across the full cyber kill chain.	RFP Clause is applicable	10	Select	0	
25	The solution should test bank's security operations, threat detection and incident response readiness capabilities.	RFP Clause is applicable	10	Select	0	
26	The solution should discover hidden elements throughout the bank's network that enable lateral movement through a single machine (once successfully within a network), which could be used to advance attacks	RFP Clause is applicable	10	Select	0	

Red Teaming Services						
S.No.	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
27	Provide risk-based prioritization of vulnerabilities that helps to focus the remediation efforts	RFP Clause is applicable	10	Select	0	
28	The solution should consist of playbooks to plan and orchestrate automated attacks on the bank's attack surface to discover and test exploitable vulnerabilities. Clarification: The solution should consist of playbooks to plan and orchestrate automated attacks on the bank's attack surface to discover and test exploitable vulnerabilities. "The solution should consist of playbooks to plan and orchestrate automated attacks on the bank's attack surface to discover and test exploitable vulnerabilities" as part of Continuous Automated Red Teaming (CART) is to achieve continuous, scalable, and riskprioritized vulnerability validation and security control testing tailored specifically to the financial sector's threat landscape. This approach transforms security testing from a periodic audit into an always-on, proactive function	RFP Clause is applicable	10	Select	0	
29	The Attack playbooks must emulate a specific adversary TTP and threat actors to test for potential risks.	Clause stands deleted.				
30	The solution must identify, analyze and prioritize digital risks from the perspective of adversaries.	RFP Clause is applicable	10	Select	0	
31	The solution should have the ability to run automated objective-based attack playbooks	RFP Clause is applicable	10	Select	0	
32	The solution should have the availability of exploits and payloads	RFP Clause is applicable	10	Select	0	
33	The solution must have the ability to create custom active attack playbooks based on Threat Intelligence of Threat Actor and their TTPs	Clause stands deleted.				
34	The solution should have the ability to schedule/run attacks based on bank's requirement.	RFP Clause is applicable	10	Select	0	
35	The solution should have the ability to run social engineering attacks, Phishing attacks, Ransomware attacks, Cloud attacks, Web application DAST attacks, Network attacks etc.	RFP Clause is applicable	10	Select	0	
36	Solution should perform assessment of security controls related to email security, WAF security and endpoint security for known vulnerabilities, misconfigurations, implementation issues and any other security gaps	Clause stands deleted.				
37	Solution should have the ability to test data loss prevention (DLP) implementation, methodology, and configuration along with other exfiltration techniques to test outbound flows of data to ensure protection of critical information Clarification: "Solution should have the ability to test data loss prevention (DLP) implementation, methodology, and configuration along with other exfiltration techniques to test outbound flows of data to ensure protection of critical information" as part of Continuous Automated Red Teaming (CART) solution test Data Loss Prevention (DLP) implementation and data exfiltration techniques is to continuously validate the organization's final line of defense against the theft of critical information. This capability ensures that all controls designed to protect sensitive data as it leaves the network are effective, regardless of the method used by the attacker	RFP Clause is applicable	10	Select	0	
38	**Reports & fixes**					
38.1	A report presenting results & conclusions of the exercise, covering technical, process and policy issues with a series of industry best-practice recommendations.	RFP Clause is applicable	10	Select	0	
38.2	Review of results and feedback in a workshop setting, to build awareness and alignment among stakeholders, and a roadmap of measures to improve security & resilience in the future.	RFP Clause is applicable	10	Select	0	
38.3	Short-term tactical fixes for immediate remediation of any outstanding vulnerabilities within the tested environments.	RFP Clause is applicable	10	Select	0	
38.4	Vulnerability report with mitigation plan and recommendations.	RFP Clause is applicable	10	Select	0	
38.5	Long-term strategic initiatives that will proactively thwart any potential repetition of vulnerabilities discovered during the exercise.	RFP Clause is applicable	10	Select	0	
TOTAL MARKS			**390**		**0**	

Threat Hunting Services					
S.No.	**Required Functionalities/Features**	**Maximum Marks**	**Compliance (S/C)**	**Calculated Score**	**Remarks**
1	To proactively search through Bank's network to detect and isolate advanced threats that evade Bank's existing security solutions.	10	Select	0	
2	Collect logs from key log sources in co-ordination with the bank.	10	Select	0	
3	Create use-cases correlation rules specific to client's environment and event sources.	10	Select	0	
4	Analyze logs for indicators of compromise such as Command.	10	Select	0	
5	Control (Command and Control - CAC) Channels, malicious IPs & websites, Geo map analysis for presence of malicious programs.	10	Select	0	
6	Analysis of logs to identify anomalous behavior/suspicious events.	10	Select	0	
7	Review and confirm observations with the client's security team.	10	Select	0	
8	Eliminate false positives.	10	Select	0	
9	Review effectiveness of SOC to detect similar events..	10	Select	0	
10	Report containing compromised hosts, malware infections, presence of bots, CAC communications and other indicators of suspicious activities	10	Select	0	
11	Threat Hunting shall also address the Detect anomalous attacks, especially low-and-slow attacks that may be happening.	10	Select	0	
12	Threat Hunting shall also address the following Identify if the attack was detected by SOC.	10	Select	0	
13	Threat Hunting shall also address the following If the SOC has detected the attack, then identify the reasons for no action being taken if the SOC has not detected the attack, then identify if an existing correlation rule requires tuning or if a new correlation rule is required or if a new solution is required.	10	Select	0	
14	Alerts on anomalous attacks in the network and recommendations for detecting and preventing such attacks in the future.	10	Select	0	
15	Bidder should be able to identify and report to the bank if access to blocked ports on a webserver is sought by an external user.	10	Select	0	
TOTAL MARKS		**150**		**0**	

Attack Surafce Management						
S.No.	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
1	All data provided by the solution or accessible on the solution by the bank should be collated from the public domain and other forums via passive/non-intrusive scans, and other non-intrusive activities	RFP Clause is applicable	10	Select	0	
2	The data gathering activity should be performed daily/frequently and updated in the solution	RFP Clause is applicable	10	Select	0	
3	Solution should store historical information about bank to provide cybersecurity maturity over time	RFP Clause is applicable	10	Select	0	
4	Solution should use comprehensive technology, manual review or other mechanisms to reduce the false positives within the dataset	RFP Clause is applicable	10	Select	0	
5	Solution should make use of visual representations and dashboards to summarise and present insights and findings related to the bank	RFP Clause is applicable	10	Select	0	
6	The visual representations should be downloadable in PDF, JPG, PNG and other generally used formats	RFP Clause is applicable	10	Select	0	
7	The individual sections of the solution should offer export of the presented data in PDF, excel and other formats	RFP Clause is applicable	10	Select	0	
8	The solution shall provide information on vulnerabilities, misconfigurations, insecure configurations, obsolete or unsupported technologies, applications, services, URLs, ports, network components, systems, databases and other relevant infrastructure that are publicly exposed or otherwise identifiable through authorized discovery and assessment activities.	The solution shall provide information on vulnerabilities, misconfigurations, insecure configurations, obsolete or unsupported technologies, services, URLs, ports and other relevant infrastructure that are publicly exposed or otherwise identifiable through authorized discovery and assessment activities.	10	Select	0	
9	The solution should provide data/information on security flaws/ inherent vulnerabilities (allegedly) reported about the digital products exposed to the Internet (For example: internet banking, mobile applications) offered to the bank's customers, as leaked in public domain, or other forums	RFP Clause is applicable	10	Select	0	
10	The solution shall identify and provide relevant information on potentially exposed sensitive information associated with the Bank, including source-code references, code snippets, API information, credentials, keys and other security-relevant information, where such information is identifiable through publicly available sources, external attack-surface intelligence or other authorized discovery mechanisms.	Deleted				
11	The solution should provide information on inventory of IT assets related to the bank and third parties associated with the bank	RFP Clause is applicable	10	Select	0	
12	The solution should provide the functionality to tag certain results or observations, to be reviewed or accessed again later	RFP Clause is applicable	10	Select	0	
13	The solution should have the option to configure triggers/notifications for certain events or developments as per bank's requirement	RFP Clause is applicable	10	Select	0	
14	All the software modules of the proposed solution should be latest as well as stable one and must have a general release date prior to the date of the submission of the proposal	Deleted				
15	There shall be a provision to manage user accounts for all personnel using the proposed solution, with functionalities to create, edit and delete user profiles, setup and reset passwords and other authentication factors using an administrator account, and assign the varying levels of access as deemed appropriate	RFP Clause is applicable	10	Select	0	
16	The solution should log all user activity which should be available for review and auditing purpose	RFP Clause is applicable	10	Select	0	
17	The solution should provide the option to pull data from it using APIs to integrate/ assimilate into another solution used by the bank	RFP Clause is applicable	10	Select	0	
18	To have a scoring/ rating mechanism to assess the cyber posture of the bank, based on the frequency required by the bank	RFP Clause is applicable	10	Select	0	
19	To be able to categorize risks (such as high/ medium/ low) as per the risk posture arrived by the model	RFP Clause is applicable	10	Select	0	
20	The solution should automatically discover the bank's assets exposed to internet, including the assets of all the entities owned by and related to bank such as overseas branches, subsidiaries, third-parties, mergers, acquisitions etc.	RFP Clause is applicable	10	Select	0	
21	The solution should discover inventory of known and unknown assets of bank, metadata, shadow IT assets and check for possible attack vectors, discover new seeds which may lead to attack surface.	RFP Clause is applicable	10	Select	0	
22	The solution must allow the input of additional entities associated with the organization directly through the console, if required by the bank	RFP Clause is applicable	10	Select	0	
23	The solution must allow the ability to remove, or unaffiliate, assets directly in the console	RFP Clause is applicable	10	Select	0	
24	The solution must allow the organization to define the prioritization of assets based upon impact of the asset	RFP Clause is applicable	10	Select	0	
25	Solution should support IPV6 entities in the process of asset discovery	RFP Clause is applicable	10	Select	0	
26	Solution must provide a workflow to define and manage state of discovered entities which affects the priority of the entity.	RFP Clause is applicable	10	Select	0	
27	Solution should have the facility to search for specific entities (based on IP, Hostname, Network or Service)	RFP Clause is applicable	10	Select	0	

Attack Surafce Management						
S.No.	**Required Functionalities/Features**	**Updated in Addendum**	**Maximum Marks**	**Compliance (S/C)**	**Calculated Score**	**Remarks**
28	Solution should provide advanced search capabilities allowing the user to filter results with AND/OR logic along with nested logic	RFP Clause is applicable	10	Select	0	
29	Solution must include metadata and discovery artifacts associated with targets	RFP Clause is applicable	10	Select	0	
30	Solution should provide detection/discovery path(s) related to entities	RFP Clause is applicable	10	Select	0	
31	Solution must illustrate changes to the attack surface of bank over time	RFP Clause is applicable	10	Select	0	
32	The solution shall correlate relevant emerging threat information with the Bank's identified external attack surface and highlight potentially affected assets and associated risks.	RFP Clause is applicable	10	Select	0	
33	Solution should have the ability to compare customer asset list (e.g., domains, hostnames, IPs, networks) in CSV format or CMDB, against discovered entities by solution and highlight differences in console	RFP Clause is applicable	10	Select	0	
34	Solution should have the feature to create policy to automatically take action based on criteria	RFP Clause is applicable	10	Select	0	
35	Solution should have the feature to automatically create help desk ticket containing asset meta data, comments, link back to the solution console and guidance. Ticket status should be automatically reflected in ASM console.	Solution should have the feature to automatically create help desk ticket containing asset meta data, comments, link back to the solution console and guidance.	10	Select	0	
36	The solution shall provide the capability to identify and classify shadow IT and unknown assets and facilitate their assessment through integration with the Bank's Vulnerability Management solution or other assessment solution available with the bank	RFP Clause is applicable	10	Select	0	
37	The solution shall support exchange of relevant asset, risk, scoring and vulnerability information with the Bank's Vulnerability Management solution through supported APIs or integration mechanisms	RFP Clause is applicable	10	Select	0	
38	Solution must have bi-directional, writetable API's that allow the organization to integrate data into the organization's existing security	Solution must have APIs that allow the organization to integrate data into the organization's existing security.	10	Select	0	
39	Solution must have facility to send notifications when a significant change in bank's attack surface occurs	RFP Clause is applicable	10	Select	0	
40	Solution must have facility to send periodic notifications summarizing changes to the bank's attack surface	RFP Clause is applicable	10	Select	0	
41	The core solution shall not require installation of dedicated hardware or software agents on the Bank's Internet-facing assets for external attack-surface discovery and monitoring. Where required, optional connectors or integrations may be used for authorized data exchange with enterprise systems.	RFP Clause is applicable	10	Select	0	
42	The solution shall support Multi-Factor Authentication (MFA), role-based access control and integration with enterprise identity providers of the bank	RFP Clause is applicable	10	Select	0	
TOTAL MARKS			**400**		**0**	

Breach Attack Simulation					
S.No.	**Required Functionalities/Features**	**Maximum Marks**	**Compliance (S/C)**	**Calculated Score**	**Remarks**
1	The solution should simulate Ransomware Attacks	10	Select	0	
2	The solution should have the ability to launch attacks using dynamically generated initial payloads with no knowns signatures across the complete cyber attack kill chain including MITRE ATT&CK complete framework (e.g. infiltration, lateral movement, exfiltration etc) with automated cleanup and restoration mechanisms	10	Select	0	
3	The ability to simulate infiltration techniques for breaching a network or infecting a host	10	Select	0	
4	The ability to simulate Machine-based attacks - known vulnerabilities on internet-facing systems, misconfiguration of network perimeter controls, exposed applications, etc.	10	Select	0	
5	The solution should identify vulnerabilities and configurations gaps across the complete threat landscape of the bank's infrastructure	10	Select	0	
6	The solutions should test Security Operations Center (SOC) detection capability of bank by simulating multi-chained payloads with advanced evasion methods including DLL Hijacking, Process Injection, and PPID spoofing for breaching and infiltrating the network.	10	Select	0	
7	The solution should have the ability to create custom use cases / simulations attacks according to bank's requirement.	10	Select	0	
8	The solution must allow the execution of simulations on multiple agents simulataneously. An attack chain must be executed on multiple endpoints agents at the same time to provide unique attack specific insights across the deployed agents in the organisation.	10	Select	0	
9	The solution must provide detailed steps, Indicators of Compromise, IoBs for all the simulation activity performed including but not limited to Process Creation, Service Creation, File Downloads, Network Connection, WMI Queries, Registry Key Modifications, Command Execution, and new threads created with appropriate data to track the attack timeline.	10	Select	0	
10	The solution should provide a detailed report on the vulnerabilities/security gaps identified through automated red teaming and summarized report which can be downloaded in PDF, Excel, CSV, Word formats.	10	Select	0	
11	The solution should support technical integrations with bank’s existing solutions (e.g., SIEMs, ticketing systems, log management, Firewalls, automation/orchestration, analytics solutions, threat intelligence solutions, etc.)	10	Select	0	
TOTAL MARKS		**110**		**0**	

Digital risk management					
S.No.	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
1	Anti-phishing and domain monitoring services	10	Select	0	
2	Social media threat protection services	10	Select	0	
3	The Bidder should report the Bank within 1 hour of detection of phishing/brand abuse website/rogue application with action plan on taking down and other alternative response mechanisms upon Bank's confirmation. The Bidder should be able to take down/shut down the phishing/brand abuse website/rogue application within agreed SLA upon Bank's confirmation, irrespective of geography	10	Select	0	
4	The Bidder should not face obstruction in their activity regardless of international border & language	10	Select	0	
5	The Service should support Unlimited takedowns of phishing sites, brand abuse and rogue apps during contract period. The Bidder should be capable of blocking of the phishing sites in web browsers.	10	Select	0	
6	Bring down the reactivated phishing site at earliest which was earlier detected as phishing site	10	Select	0	
7	The Bidder should track new domain name registrations to detect any spoofed site being Registered	10	Select	0	
8	Identification of account impersonation activity	10	Select	0	
9	The Bidder should be able to coordinate with regulatory/law enforcement agencies like CERT-IN/Cyber Crime Cells / RBI/Third Party Auditors	10	Select	0	
10	The Bidder should have global partnership with domain name registrars, application distribution platforms and ISPs for easier take downs of phishing sites & rogue apps anywhere in the world.	10	Select	0	
11	The Bidder should monitor any fraudulent mobile applications targeting Bank Bank's customers to capture their credentials for fraudulent transactions	10	Select	0	
12	The Bidder should have ability to detect potential Infringements and malicious websites by use of contemporary convergent technologies like threat intelligence, ML etc.	10	Select	0	
13	The Bidder should monitor and log all phishing attempts	10	Select	0	
14	The Bidder should monitor networks known to be source of attacks and/or points of collection of compromised data, compromised devices, Malicious URL's, malicious command and control sites	10	Select	0	
15	The Bidder should be able to support shutting down/blocking of Trojans, malware, phishing sites irrespective of region of origin or browsers or ISPs.	10	Select	0	
16	The Bidder should monitor similar domain name registrations	10	Select	0	
17	The Bidder should provide weekly, monthly & quarterly reports to the bank via email. Additionally, whenever incidents are reported/resolved, bank is to be notified via email	10	Select	0	
18	Use Digital watermarking to detect phishing sites	10	Select	0	
19	Provide alert on detection of Phishing website which include IP address, URL and domain	10	Select	0	
20	Identify if any of the employees or end-customers have been phished via the phishing campaigns	10	Select	0	
21	Monitoring all major mobile app marketplaces for counterfeit, copycat apps, or apps infringing trademarks	10	Select	0	
22	The Bidder should have the capability for 24x7x365 detection and monitoring for brand abuse attacks and rogue apps targeting the Bank (logo, URL Domain, digital watermark etc.)	10	Select	0	
23	Monitor for Brand mentions in sources Messaging platforms like Telegram, Discord, Facebook, Twitter, Instagram etc. (if any)	10	Select	0	
24	Monitoring potential logo abuse for organization logo (if any)	10	Select	0	
25	Perform brand monitoring and protection including a variety of sources, feeds, locations, and repositories, but not limited to: i. Malicious Website/URL Scanning iii. DNS Suite (Domain Name Service) Brand Suite iv. Social Suite – Social media platforms, Blogs, Forums v. Fake domains similar to bank's domain	10	Select	0	
26	The bidder should comply with time-to-time advisories which is specific to Brand Monitoring Services. It should make any necessary changes in the services accordingly and provide updated services without any additional cost.	10	Select	0	
27	The platform should offer Top Executives/VIP account monitoring	10	Select	0	
28	The platform should be able to identify account impersonation	10	Select	0	
29	The platform should be able to identify any fake apps /sites / scam / misinformation in the name of Company has to be identified by the tool and reported to the bank.	10	Select	0	
30	The Bidder should conduct analysis of social networks such as Facebook, Twitter, Linked-in etc. and domain registrations to find fake social profiles, malicious mentions and similar domains that impersonate the bank to compromise customer information.	10	Select	0	
31	The Bidder should be able to provide brand abuse support services-for Bank's public websites, Internet facing websites, mobiles applications and social media accounts	10	Select	0	
32	Anti-phishing and domain monitoring services	10	Select	0	
33	Compliance with regulatory advisory on phishing attacks	10	Select	0	

Digital risk management					
S.No.	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
34	Brand abuse services	10	Select	0	
35	Social media threat protection services	10	Select	0	
36	Monitoring of rogue apps on AppStore like Google Play, Apple Store etc. (if any) The Bidder should ensure that the service must not hamper working of Bank's websites or Apps.	10	Select	0	
37	The Bidder should report the Bank within 1 hour of detection of phishing/brand abuse website/rogue application with action plan on taking down and other alternative response mechanisms upon Bank's confirmation. The Bidder should be able to take down/shut down the phishing/brand abuse website/rogue application within agreed SLA upon Bank's confirmation, irrespective of geography	10	Select	0	
38	The Bidder should not face obstruction in their activity regardless of international border & language	10	Select	0	
39	The Service should support takedown actions through relevant platforms for identified Brand Abuse/Brand Impersonation assets and rogue applications during the contract period.	10	Select	0	
40	Bring down the reactivated phishing site at earliest which was earlier detected as phishing site	10	Select	0	
41	The Bidder should track new domain name registrations to detect any spoofed site being Registered	10	Select	0	
42	Identify any fake apps / sites / scam / misinformation in the name of Company.	10	Select	0	
43	Identification of account impersonation activity	10	Select	0	
44	The Bidder should be able to coordinate with regulatory/law enforcement agencies like CERT-IN/Cyber Crime Cells / RBI/Third Party Auditors	10	Select	0	
45	The Bidder/OEM should be member of Anti-Phishing Working Group (APWG) or an equivalent international cybersecurity industry affiliation.	10	Select	0	
46	The Bidder should have global partnership with domain name registrars, application distribution platforms and ISPs for easier take downs of phishing sites & rogue apps anywhere in the world.	10	Select	0	
47	The Bidder should monitor any fraudulent mobile applications targeting Bank Bank's customers to capture their credentials for fraudulent transactions	10	Select	0	
48	The Bidder should provide for identification of fake recruitment schemes claiming affiliation with the Bank	10	Select	0	
49	The Bidder should have ability to detect potential Infringements and malicious websites by use of contemporary convergent technologies like threat intelligence, ML etc.	10	Select	0	
50	The Bidder should monitor and log all pharming and phishing attempts	10	Select	0	
51	The Bidder should monitor networks known to be source of attacks and/or points of collection of compromised data, compromised devices, Malicious URL's, malicious command and control sites	10	Select	0	
52	The Bidder should be able to support shutting down/blocking of Trojans, malware, phishing sites irrespective of region of origin or browsers or ISPs.	10	Select	0	
53	The Bidder should monitor similar domain name registrations	10	Select	0	
54	The Bidder should provide weekly, monthly & quarterly reports to the bank via email. Additionally, whenever incidents are reported/resolved, bank is to be notified via email	10	Select	0	
55	**Bidder should be able to take counter measures including (but not limited to)**				
55.1	Bring websites down that are capable of causing phishing attacks	10	Select	0	
55.2	Baiting	10	Select	0	
55.3	Notify various internet browsers about detected sites for blocking these at browser level.	10	Select	0	
55.4	The solution shall continuously monitor the Bank's external digital footprint for fraudulent or unauthorized online listings, impersonation, phishing, fake websites/domains, and other digital brand-abuse activities that may mislead customers, and shall support timely detection, validation, alerting, and takedown/remediation of identified threats.	10	Select	0	
55.5	Prompt submission of enforcement notices and for the removal of rogue or infringing applications	10	Select	0	
55.6	Bidder must have capability for monitoring of look-alike domain name registrations and alerting the Bank in case of detection	10	Select	0	
55.7	The Bidder should support wide coverage of web, social media and email sources to detect newly configured phishing attacks, often before or as soon as they are fully launched.	10	Select	0	
55.8	Solution should be able to identify potential brand infringements and affiliations risk related to misuse of bank's logo on 3rd party website.	10	Select	0	
56	**Reporting & Dashboard**				
56.1	The bidder should provide reports to various target users of bank such as leadership team, senior management, security operations team etc. as per defined frequency	10	Select	0	
56.2	The Bidder should provide weekly, monthly & quarterly reports to the bank via email. Additionally, whenever incidents are reported/resolved, bank is to be notified via email	10	Select	0	
56.3	The bidder should provide a summarized report to senior management on the identified findings as per bank's requirement	10	Select	0	
TOTAL MARKS		**650**		**0**	

Dark Web Monitoring						
S.No.	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
1	The proposed solution shall continuously monitor, collect, correlate and provide automated alerting, reporting and threat intelligence from Clear Web, Deep Web, Dark Web, underground forums, messaging platforms and other publicly accessible intelligence sources	RFP Clause is applicable	10	Select	0	
2	The solution shall detect and notify exposure or leakage of confidential documents, sensitive files, internal documents, intellectual property and organizational information	RFP Clause is applicable	10	Select	0	
3	The solution shall provide contextual threat intelligence including Threat Actors, Campaigns, TTPs, malware families, attribution (where available), Indicators of Compromise (IOCs), attack trends and associated intelligence.	RFP Clause is applicable	10	Select	0	
4	The solution shall provide advanced search capabilities through GUI and APIs using keywords, Threat Actors, Malware Families, Campaigns, CVEs, TTPs, C2 Infrastructure, IOCs, Countries and Industry sectors.	RFP Clause is applicable	10	Select	0	
5	The solution shall identify exploit proof-of-concepts, exploit discussions, exploit kits, weaponization trends and emerging exploit intelligence associated with vulnerabilities.	RFP Clause is applicable	10	Select	0	
6	The solution shall maintain historical intelligence of Threat Actors, Campaigns, Malware, Domains, URLs, IP Addresses, Hashes and Infrastructure.	RFP Clause is applicable	10	Select	0	
7	The solution shall continuously monitor cyber threats associated with the Bank, subsidiaries, overseas branches, brands, third parties and digital assets.	RFP Clause is applicable	10	Select	0	
8	Detect exposure of confidential documents, intellectual property, sensitive files and organizational information.	RFP Clause is applicable	10	Select	0	
9	Monitor targeted attacks, threat discussions, planned attacks and references related to the Bank.	RFP Clause is applicable	10	Select	0	
10	Monitor cyber threats affecting Banking, Financial Services, Insurance and Payment ecosystems.	RFP Clause is applicable	10	Select	0	
11	Detect leaked credentials including usernames, passwords, session tokens, cookies, API Keys and Secrets.	RFP Clause is applicable	10	Select	0	
12	Detect ransomware, extortion, fraud campaigns and direct threats targeting the organization.	RFP Clause is applicable	10	Select	0	
13	Monitor brand abuse, impersonation and digital identity misuse.	RFP Clause is applicable	10	Select	0	
14	Monitor Internet Banking, Mobile Banking, APIs, payment systems and customer-facing applications.	RFP Clause is applicable	10	Select	0	
15	Detect exposed servers, cloud assets, VPNs, certificates and Internet-facing infrastructure.	RFP Clause is applicable	10	Select	0	
16	Monitor IPs, Domains, DNS, Certificates and Internet-facing assets.	RFP Clause is applicable	10	Select	0	
17	Monitor domains, brands, executives and organizational assets.	RFP Clause is applicable	10	Select	0	
18	Monitor fraudulent social media accounts and impersonation.	RFP Clause is applicable	10	Select	0	
19	Monitor sector-specific cyber threats relevant to Banking.	RFP Clause is applicable	10	Select	0	
20	Detect typo-squatted, homoglyph and phishing domains.	RFP Clause is applicable	10	Select	0	
21	Monitor suspicious SSL/TLS certificate issuance.	RFP Clause is applicable	10	Select	0	
22	Provide WHOIS, DNS and Domain Registration Intelligence.	RFP Clause is applicable	10	Select	0	
23	Monitor phishing infrastructure, fake domains and C2 hosting.	RFP Clause is applicable	10	Select	0	
24	Monitor MX, SPF, DKIM and DMARC changes for suspicious domains.	RFP Clause is applicable	10	Select	0	
25	Provide Passive DNS intelligence and historical DNS resolution.	RFP Clause is applicable	10	Select	0	
26	Detect leaked payment data, customer information and sensitive organizational data.	RFP Clause is applicable	10	Select	0	
27	Monitor Clear Web, Deep Web and Dark Web for leaked credentials, payment information, documents, APIs and sensitive data with automated alerts.	RFP Clause is applicable	10	Select	0	
28	The solution shall collect intelligence from the following, not limited to:					
28.1	Domain Intelligence	RFP Clause is applicable	10	Select	0	
28.2	Hacker Forums	RFP Clause is applicable	10	Select	0	
28.3	IRC	RFP Clause is applicable	10	Select	0	
28.4	Public intelligence sources	RFP Clause is applicable	10	Select	0	
28.5	Web Logs	Deleted				
28.6	IP Feed	RFP Clause is applicable	10	Select	0	
28.7	Breach Repository/Credential Intelligence	RFP Clause is applicable	10	Select	0	
28.8	Payment intelligence	RFP Clause is applicable	10	Select	0	
28.9	Credit Card Store	RFP Clause is applicable	10	Select	0	
28.10	Compromised Credentials	RFP Clause is applicable	10	Select	0	
28.11	Brand Intelligence	RFP Clause is applicable	10	Select	0	
28.12	Malware Repositories	RFP Clause is applicable	10	Select	0	
29	Detect organizational and customer data breaches from monitored sources.	RFP Clause is applicable	10	Select	0	
30	Support multilingual intelligence collection across global geographies.	RFP Clause is applicable	10	Select	0	
31	Utilize AI/ML, analytics, heuristics and analyst validation to improve detection accuracy and reduce false positives.	RFP Clause is applicable	10	Select	0	
32	Monitor public security communities and intelligence sources.	RFP Clause is applicable	10	Select	0	
33	Detect fraudulent mobile applications across major application marketplaces.	RFP Clause is applicable	10	Select	0	
34	Monitor newly registered domains impersonating the Bank.	RFP Clause is applicable	10	Select	0	
35	Support coordination with CERT-In, RBI, Law Enforcement Agency(LEA) and authorized agencies.	RFP Clause is applicable	10	Select	0	

Dark Web Monitoring						
S.No.	Required Functionalities/Features	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
36	Detect fraudulent mobile applications targeting customers.	RFP Clause is applicable	10	Select	0	
37	Provide searchable knowledge base, advisories and FAQs.	RFP Clause is applicable	10	Select	0	
38	Detect exploit discussions and exploit intelligence for technologies used by the Bank.	RFP Clause is applicable	10	Select	0	
39	Utilize Threat Intelligence, AI/ML and analytics for phishing, fraud and malicious website detection.	RFP Clause is applicable	10	Select	0	
40	Monitor C2 infrastructure, malware hosting, phishing infrastructure and botnets.	RFP Clause is applicable	10	Select	0	
41	Takedown for phishing sites, malicious domains and rogue applications	RFP Clause is applicable	10	Select	0	
42	Continuously monitor look-alike and typo-squatted domains.	RFP Clause is applicable	10	Select	0	
43	Provide scheduled and on-demand Executive, Operational and Technical reports with configurable frequency.	RFP Clause is applicable	10	Select	0	
44	Support Email, SMS, and other notifications based on configurable severity.	RFP Clause is applicable	10	Select	0	
45	Correlate intelligence across Tor, Onion, Dark Web, ransomware leak sites, underground forums, messaging platforms, criminal marketplaces and emerging communication channels.	RFP Clause is applicable	10	Select	0	
46	Detect leaked credentials, API Keys, OAuth Tokens, SSH Keys, Digital Certificates, cryptographic secrets and cloud access keys associated with the Bank.	RFP Clause is applicable	10	Select	0	
47	Monitor exposed customer information, payment card data, PII, confidential documents, intellectual property, source code and sensitive organizational data	RFP Clause is applicable	10	Select	0	
48	Correlate intelligence with MITRE ATT&CK techniques, malware families, threat actors, campaigns and Indicators of Compromise (IOCs).	RFP Clause is applicable	10	Select	0	
49	Support enrichment using CVE, CVSS v4.0, EPSS, CISA Known Exploited Vulnerabilities (KEV) and other industry-recognized threat intelligence sources.	RFP Clause is applicable	10	Select	0	
50	Monitor and identify supply-chain threats affecting the Bank and critical third-party vendors.	RFP Clause is applicable	10	Select	0	
51	The solution shall monitor public code repositories, open cloud storage repositories, and other publicly accessible sources for exposed source code, email addresses, IP addresses, passwords, access keys, and other organizational information.	RFP Clause is applicable	10	Select	0	
52	The solution shall support initiation and management of takedown requests for phishing websites, typosquatting domains, and rogue mobile applications. The required takedown licenses shall be provided from Day One as specified by the Bank.	RFP Clause is applicable	10	Select	0	
53	The solution shall discover leaked data across the dark web, including sensitive files, financial data, payment card data, PII, and compromised credentials, and identify the source of the data breach, including third-party sources, where available.	RFP Clause is applicable	10	Select	0	
TOTAL MARKS			630		0	

Phishing Simulation						
S.No.	**Required Functionalities/Features**	**Updated in Addendum**	**Maximum Marks**	**Compliance (S/C)**	**Calculated Score**	**Remarks**
1	The platform shall facilitate creation of phishing campaigns including QR code phishing which can be customized by bank.	RFP Clause is applicable	10	Select	0	
2	The platform should include in-built email templates based on banking environment, current events and previous successful attacks.	RFP Clause is applicable	10	Select	0	
3	The platform should support creation of new templates and customization as per bank's requirement.	RFP Clause is applicable	10	Select	0	
4	The platform should provide capability to include specific target employees to whom the campaign needs to be executed.	RFP Clause is applicable	10	Select	0	
5	The platform should support scaling to target unlimited number of email IDs for a campaign.	RFP Clause is applicable	10	Select	0	
6	The platform should be scalable in terms of number of campaigns and frequency of the activity performed through the platform.	RFP Clause is applicable	10	Select	0	
7	The platform shall have the capability to schedule the campaign for a future date and time.	RFP Clause is applicable	10	Select	0	
8	The platform should have capability to install a plugin with the bank's email client for reporting of any phishing incident.	RFP Clause is applicable	10	Select	0	
9	The platform should support English language and for creating phishing templates. Support in other regional languages and Hindi would be an added advantage.	RFP Clause is applicable	10	Select	0	
10	The platform should allow creation of multiple users for executing the campaigns.	RFP Clause is applicable	10	Select	0	
11	The platform should support integration with bank's active directory.	RFP Clause is applicable	10	Select	0	
12	The proposed solution should have incident management capabilities and same should be integrated with Bank's Incident Management solution.	RFP Clause is applicable	10	Select	0	
13	The platform should support integration with bank's security stack such as SIEM, SOAR, data lake etc., as per bank's requirement.	RFP Clause is applicable	10	Select	0	
14	The bidder shall be capable of performing vishing exercises in both automated and manual methods. The automated approach shall support scalability in conducting vishing campaigns through Bidder's infrastructure/gateway. For conducting vishing using manual approach, each exercise shall be targeted for 100 employees per month.	RFP Clause is applicable	10	Select	0	
15	The bidder shall be capable to perform vishing activity in multiple regional languages, covering minimum English and Hindi.	RFP Clause is applicable	10	Select	0	
16	The bidder shall conduct Smishing exercises based on the frequency and number of target employees defined by the Bank. The bidder shall provide, maintain and manage an independent SMS gateway to perform smishing activity as per bank's requirement. The bidder shall maintain adequate security measures to protect Bank's data including any PII information submitted by users during the activity.	RFP Clause is applicable	10	Select	0	
17	The bidder shall include relevant phishing, vishing and smishing templates based on current threat landscape targeted to banking environment.	RFP Clause is applicable	10	Select	0	
18	Bidder shall ensure that there is no restriction in number of phishing emails, number of calls, number of SMS to perform simulated phishing, vishing, smishing.	RFP Clause is applicable	10	Select	0	
19	Phishing/Vishing/Smishing/Qrishing simulation exercises to be conducted using any of the following methods, as per Bank's requirement:					
19.1	**E-Mail Phishing Simulation Exercise**					
a	Creating Mock E-mails: Develop customized email templates based on identified phishing scenarios.	RFP Clause is applicable	10	Select	0	
b	Developing of look-alike website/portal.	RFP Clause is applicable	10	Select	0	
c	Choose landing page: Design a webpage to be redirected from the phishing. email and to capture the user information/ credentials in encrypted form.	RFP Clause is applicable	10	Select	0	
d	Categorize and prioritize the delivery mechanism.	RFP Clause is applicable	10	Select	0	
e	Testing the servers and filters: Check if the servers and filters are bypassed for simulation.	RFP Clause is applicable	10	Select	0	
f	Pilot Testing: Perform the pilot test by sending emails to selected employees.	RFP Clause is applicable	10	Select	0	
g	Launch the mock attack: deploy the main phishing assessment to the target users.	RFP Clause is applicable	10	Select	0	
h	Monitoring- for phishing email delivery, response to phishing email, progress of phishing campaign.	RFP Clause is applicable	10	Select	0	
19.2	**Phishing simulation exercise through Vishing**					
a	Developing infrastructure for vishing attack.	RFP Clause is applicable	10	Select	0	
b	Creating Vishing Scenarios.	RFP Clause is applicable	10	Select	0	
c	Conducting Vishing exercise.	RFP Clause is applicable	10	Select	0	
d	Collect the information about vished users.	RFP Clause is applicable	10	Select	0	
e	Capturing of Vishing responses received from the targeted employee.	RFP Clause is applicable	10	Select	0	
f	Executables for Vishing attack need to be provided by the Bidder.	RFP Clause is applicable	10	Select	0	
g	Vendor shall arrange Server and other infrastructure for the exercise at their own cost.	RFP Clause is applicable	10	Select	0	
19.3	**Phishing simulation exercise through Mobile**					
a	Developing look alike mobile application (Android and IOS) for phishing attack.	RFP Clause is applicable	10	Select	0	
b	Categorize and prioritize the delivery mechanism.	RFP Clause is applicable	10	Select	0	
c	Hosting the phishing mobile application for the exercise in Vendor's Location.	RFP Clause is applicable	10	Select	0	
d	Conducting Mobile Phishing exercise.	RFP Clause is applicable	10	Select	0	
e	Reports & Statistics: Generate the report at the end of simulation and presentation to Management.	RFP Clause is applicable	10	Select	0	

Phishing Simulation						
S.No.	**Required Functionalities/Features**	**Updated in Addendum**	**Maximum Marks**	**Compliance (S/C)**	**Calculated Score**	**Remarks**
f	Identifying the susceptible users and targeted awareness communications to improve the awareness level of users.	RFP Clause is applicable	10	Select	0	
g	Capturing mobile Phishing responses received from the targeted employee.	RFP Clause is applicable	10	Select	0	
h	Executables for Phishing attack need to be provided by the Bidder.	RFP Clause is applicable	10	Select	0	
i	Vendor shall arrange Server and other infrastructure for the exercise at their own cost.	RFP Clause is applicable	10	Select	0	
19.4	**Quishing simulation exercise**					
a	creation of phishing campaigns including QR code phishing which can be customized by bank.	RFP Clause is applicable	10	Select	0	
19.5	**Smishing simulation exercise**					
a	Conduct simulated Smishing Exercises as per the requirement of the Bank	RFP Clause is applicable	10	Select	0	
b	Capturing statistics to measure smishing exercises	RFP Clause is applicable	10	Select	0	
c	Phishing, vishing and smishing templates based on current threat landscape targeted to banking environment	RFP Clause is applicable	10	Select	0	
20	**Reporting and Dashboard**					
20.1	A detailed report presenting results, key learning & conclusions of the exercise, covering technical, process and policy issues with a series of industry best-practice recommendations, response of the targeted employees (e.g. Delivered, opened, clicked etc.) and user data/ credential collected of employees through phishing simulation. The same may be required to be presented before Senior Management /Committee.	RFP Clause is applicable	10	Select	0	
20.2	Review of results and feedback in a workshop setting, to build awareness among employees, and a roadmap of measures to improve awareness among employees.	RFP Clause is applicable	10	Select	0	
20.3	Progress report comparison to previous exercises in the year.	RFP Clause is applicable	10	Select	0	
20.4	Communication to all targeted employees through email for their response to phishing simulation exercise & future guidelines.	RFP Clause is applicable	10	Select	0	
20.5	Info Graphics of Key-indicators to identify phishing e-mail, present in the e-mail sent to targeted employees during the simulation exercise, to be provided within 3 days of completion of exercise.	RFP Clause is applicable	10	Select	0	
21	**Training**					
21.1	The platform should include mandatory training modules to train the employees who have been phished.	RFP Clause is applicable	10	Select	0	
21.2	The platform should force the phished employee for completion of training module available in the solution.	RFP Clause is applicable	10	Select	0	
21.3	The training modules should be customizable and flexible based on the level of the awareness of employee being phished and job role.	RFP Clause is applicable	10	Select	0	
21.4	The platform should be able to map complete lifecycle of cyber awareness process of each user and represent the same information through a real-time dashboard.	RFP Clause is applicable	10	Select	0	
21.5	The platform should have the capability to randomize questions basis on the content and assess users on the same.	RFP Clause is applicable	10	Select	0	
21.6	Post completion of Cyber Awareness training module, user to undergo Cyber Awareness training Assessment to understand the effectiveness of the training program.	RFP Clause is applicable	10	Select	0	
21.7	The platform should include customized learning content such as videos, infographics, posters, wallpapers, gamification, quiz , interactive training content etc. as per bank's requirement.	RFP Clause is applicable	10	Select	0	
21.8	The platform should provide the functionality of issuing a certificate to the employees on completion of training modules.	RFP Clause is applicable	10	Select	0	
21.9	The platform should support ease of use and the training content should be engaging for end users.	RFP Clause is applicable	10	Select	0	
21.10	Bank should have a complete access to control and choose any topic of Cyber Security awareness training and should be able to assign the same to any target group desired by Bank.	RFP Clause is applicable	10	Select	0	
21.11	Cyber awareness progress should be measured to identify training pending users' departments they belong to and the impact they carry to the security posture of the Bank.	RFP Clause is applicable	10	Select	0	
21.12	In the absence of completion of training program, the platform should schedule across automated escalation to reporting stakeholders to ensure compliance and achievement of completion rate.	RFP Clause is applicable	10	Select	0	
22	**Reporting**					

Phishing Simulation						
S.No.	**Required Functionalities/Features**	**Updated in Addendum**	**Maximum Marks**	**Compliance (S/C)**	**Calculated Score**	**Remarks**
22.1	The platform should provide a detailed report/dashboard of the activities performed by the user including but not limited to the following: i. Total Campaigns ii. Total No. of users targeted iii. Total Mails Sent iv. Total Mails Opened v. Count of link clicked/QR code scanned vi. Sensitive Information Submitted vii. Trainings Completed viii. Trainings Pending ix. Number of Phishing Reported x. Click Rate by Department/location xi. Campaign Results capturing the entire campaign lifecycle	RFP Clause is applicable	10	Select	0	
22.2	The platform should provide dashboard for each phishing campaign and also facilitate access to previous campaign information.	RFP Clause is applicable	10	Select	0	
22.3	The platform should have capability to filter and pull customized reports in CSV, Excel and PDF formats.	RFP Clause is applicable	10	Select	0	
22.4	The bidder should be able to capture statistics to measure success of phishing, vishing and smishing exercises. A detailed report with campaign details and metrics shall be submitted to bank on completion of the activity.	RFP Clause is applicable	10	Select	0	
22.5	The bidder should provide reports on the latest information security trends and regulatory guidelines (if any) related to the proposed scope of work in this RFP, on a frequency mutually agreed with the bank.	RFP Clause is applicable	10	Select	0	
22.6	Results to drive from simulation should provide the number of vulnerable users and non-vulnerable users, departments they belong to and the impact they carry to the security posture of the Bank.	RFP Clause is applicable	10	Select	0	
23	**Other Requirements**					
23.1	The bidder shall perform review of Email solution twice in a year from Cert-IN empaneled organization and compliance verification shall be conducted within 2 months from the report submission.	Deleted				
23.2	The platform should provide a separate dashboard for monitoring of DMARC/DNS Monitoring for Bank's Email solution.	Deleted				
23.3	Support and Update	Deleted				
23.4	The bidder should provide 24*7 support (over call) for any kind of issue in functionality/performance/integration of the platform during the entire tenure of contract. In case, the issue is not resolved for more than 8 hours, support personnel should visit Bank's CISO Office at Mumbai or at Hyderabad to resolve the issue. The bidder shall provide the details of support team and escalation matrix for immediate assistance to bank's team for any issue.	Clause stands deleted. Clarification: Bank's project office is in Delhi NCR; DC – Mumbai and DR – Noida.				
23.5	The bidder should perform updation of new features and upgradation of on-premise platform automatically from time-to-time.	Deleted				
23.6	The bidder should provide updates/upgrades of the proposed solution at free of cost during the contract period.	RFP Clause is applicable	10	Select	0	
23.7	For Phishing activity, the bidder should not store any bank data in vendor location, data storage shall be restricted only on Bank network. The bidder should ensure that the data at rest and in motion shall be encrypted.	The Bidder/OEM shall ensure that Bank data generated or collected during the phishing simulation activities is adequately protected and shall not be used, disclosed, shared or retained by the Bidder/OEM for any purpose other than delivery of the contracted service and shall comply with the applicable data residency, security, confidentiality and regulatory requirements specified in the RFP.	10	Select	0	
23.8	For Smishing and Vishing activities, the bidder shall maintain adequate security measures to protect Bank's data including any PII information submitted by users during the activity.	RFP Clause is applicable	10	Select	0	
TOTAL MARKS			**720**		**0**	

Anti-Phishing Services						
S.No.	**Required Functionalities/Features**		**Maximum Marks**	**Compliance (S/C)**	**Calculated Score**	**Remarks**
1	Refer Digital Risk Management Solution Specifciations			Select	0	
TOTAL MARKS			**0**		**0**	

Brand abuse						
S.No.	**Required Functionalities/Features**		**Maximum Marks**	**Compliance (S/C)**	**Calculated Score**	**Remarks**
1	Refer Digital Risk Management Solution Specifciations			Select	0	
TOTAL MARKS			**0**		**0**	

SUMMARY									
S.No.	**Payment Milestone**	**Sheet Name**	**Implementation**	**Y1**	**Y2**	**Y3**	**Y4**	**Y5**	**Grand Total**
1	Product Cost	Product License Cost	0						0
2		Product Implementation cost	0						0
3	OEM Services Cost	OEM Services Cost		0	0	0	0	0	0
4	Hardware Cost	IT Infrastructure Cost	0						0
5		Appliance Cost	0						0
6	ATS & AMC	ATS/Subscription Cost		0	0	0	0	0	0
		Appliance AMC Cost						0	0
7		IT Infrastructure AMC Cost		0	0	0	0	0	0
8	Facility Management Cost	FM Cost		0	0	0	0	0	0
9	Other Cost	Other Cost		0					0
								TOTAL COST OF OWNERSHIP	0
								GST%	18%
							Total Cost (Inclusive of GST)		0
TOTAL COST OF OWNERSHIP (INCLUSIVE OF GST)									

Notes	
1	Bank will procure additional licenses, services, hardware as per the rate provided in the respective Sheets or on pro-rata basis.
2	The Bank, at its sole discretion, reserves the right to either procure the required items from the bidder or supply them from its existing inventory. However, the bidder is strictly required to submit itemized pricing for each line item without exception.
3	The Bank may procure additional quantities, as and when required, during the contract period at the unit rates quoted by the Bidder in the Price/Rate Sheet. Where the required quantity or configuration is not explicitly covered in the Price/Rate Sheet, the additional quantity shall be procured on a pro-rata basis based on the quoted rates.
4	Instructions to Fill the Summary Tab
4.1	Grand Total of **Product License Cost** sheet is to be provided/quoted in the **Implementation Column** in the BOM (Summary Tab)
4.2	Grand Total of **Product Implementation cost** sheet is to be provided/quoted in the **Implementation Column** in the BOM (Summary Tab)
4.3	Grand Total of **OEM Services Cost** sheet is to be provided/quoted in the **respective year column** in the BOM (Summary Tab)
4.4	Grand Total of **Hardware Cost** sheet is to be provided/quoted in the **Implementation Column** in the BOM (Summary Tab)
4.5	Grand Total of **Hardware AMC Cost** sheet is to be provided/quoted in the **respective year column** in the BOM (Summary Tab)
4.6	Grand Total of **Other Cost** sheet is to be provided/quoted in the **respective year column** in the BOM (Summary Tab)
4.7	Grand Total of **FM Cost** sheet is to be provided/quoted in the **respective year column** in the BOM (Summary Tab)

4.8	The Bidder shall quote all applicable costs in the respective detailed Price/Rate Sheets. The Summary Tab shall be populated strictly based on the Grand Total of the corresponding detailed Price/Rate Sheets. 1)The Bidder shall not leave any applicable price field blank. Where a particular item/component is not applicable, the Bidder shall enter “NIL” or “0”, as applicable. 2) The Bank may procure additional licences, subscriptions, services, hardware, appliances, resources or other items during the Contract period at the unit rates quoted by the Bidder in the respective Price/Rate Sheets, subject to the terms and conditions of the RFP. 3) The Bank, at its sole discretion, reserves the right to either: a) procure the required items/services from the Bidder; or b) provide/procure the same from its existing inventory or other sources. c) Notwithstanding the above, the Bidder shall mandatorily submit itemized pricing for each line item in the respective Price/Rate Sheets. The Bank may procure additional quantities, as and when required, during the Contract period at the unit rates quoted by the Bidder. Where the required quantity/configuration is not explicitly covered in the Price/Rate Sheet, the additional quantity/configuration shall be priced on a pro-rata basis using the applicable quoted rate and configuration, subject to acceptance by the Bank.
5	The rates quoted in the respective Price/Rate Sheets shall be firm and binding for the applicable period.
6	The Bidder shall ensure that the Grand Total / Total Cost of Ownership calculated in the detailed Price/Rate Sheets submitted as part of the Bid is consistent with the total price quoted on the GeM Portal. The Bidder shall mandatorily provide a detailed breakup of the GeM quoted price through the prescribed Price/Rate Sheets, including Product Licence Cost, Product Implementation Cost, OEM Services Cost, Hardware/Appliance Cost, ATS/Subscription Cost, AMC Cost, FM/O&M Cost and Other Cost
7	The Bidder shall ensure that the detailed Price/Rate Sheets provide a complete and accurate breakup of the total GeM quoted price and that all mandatory items/services required under the RFP are adequately covered within the quoted GeM price.
8	In case of any discrepancy, variation or inconsistency between the prices calculated in the individual sheets and the final price quoted on the Government e-Marketplace (GeM) portal, the final GeM price shall prevail and shall be considered final, binding and conclusive. The Bidder shall ensure that the prices/amounts quoted under each of the following sheets remain binding and consistent with the corresponding quantities and rates submitted in the bid, subject to the final price quoted on the GeM portal.

Product License Cost					
S.No.	Solution name	License Cost Solution Description	Qty	Rate (in INR)	Total (in INR)
DATA CENTER (PRODUCTION) - PRIMARY & HIGH AVAILAIBILITY					
1	Security Information and Event Management (SIEM)				0
2	Security Orchestration, Automation & Response (SOAR)				0
3	User & Entity Behaviour Analytics (UEBA)				0
4	Deception Technology (Decoy/Honeypot)				0
5	Extended Detection & Response (XDR)				0
6					
7	Threat Intelligence Platform (TIP)				0
8	Vulnerability Assessment & Management (VA)				0
9	Identity Threat Detection & Response (ITDR)				0
10	Application Security Testing (AST) Tool				0
11	Cloud Security Posture Management (CSPM)				0
12	Cloud-Native Application Protection Platform (CNAPP)				0
13	Cloud Workload Protection Platform (CWPP)				0
14	Continuous Threat Exposure Management (CTEM)				0
15	Any other, please specify				0
16	Any other, please specify				0
GRAND TOTAL DC (PRIMARY & HA)					**0**
DISASTER RECOVERY CENTER (PRODUCTION) - PRIMARY & HIGH AVAILAIBILITY					
1	Security Information and Event Management (SIEM)				0
2	Security Orchestration, Automation & Response (SOAR)				0
3	User & Entity Behaviour Analytics (UEBA)				0
4	Deception Technology (Decoy/Honeypot)				0
5	Extended Detection & Response (XDR)				0
6					
7	Threat Intelligence Platform (TIP)				0
8	Vulnerability Assessment & Management (VA)				0
9	Identity Threat Detection & Response (ITDR)				0
10	Application Security Testing (AST) Tool				0
11	Cloud Security Posture Management (CSPM)				0
12	Cloud-Native Application Protection Platform (CNAPP)				0
13	Cloud Workload Protection Platform (CWPP)				0
14	Continuous Threat Exposure Management (CTEM)				0
15	Any other, please specify				0
16	Any other, please specify				0
GRAND TOTAL DR (PRIMARY & HA)					**0**
NON-PRODUCTION					
1	Security Information and Event Management (SIEM)				0
2	Security Orchestration, Automation & Response (SOAR)				0
3	User & Entity Behaviour Analytics (UEBA)				0

Product License Cost					
S.No.	Solution name	License Cost Solution Description	Qty	Rate (in INR)	Total (in INR)
4	Deception Technology (Decoy/Honeypot)				0
5	Extended Detection & Response (XDR)				0
6					
7	Threat Intelligence Platform (TIP)				0
8	Vulnerability Assessment & Management (VA)				0
9	Identity Threat Detection & Response (ITDR)				0
10	Application Security Testing (AST) Tool				0
11	Cloud Security Posture Management (CSPM)				0
12	Cloud-Native Application Protection Platform (CNAPP)				0
13	Cloud Workload Protection Platform (CWPP)				0
14	Continuous Threat Exposure Management (CTEM)				0
15	Any other, please specify				0
16	Any other, please specify				0
GRAND TOTAL NON-PRODUCTION					0
GRAND TOTAL					0

Notes	
Note 1	Bidder to provide the following information in the ***Solution Description*** column for each of the proposed product/solution for respective environment: 1. Make of the Solution 2. Model of the solution 3. Version of the proposed solution 4. Edition 5. Licensing Metrics
Note 2	Qty proposed by the bidder should be inline with the Licensing Metrics of the respective solution example If Licensing metrics of SIEM is EPS Count then QTY should mentioned 75000 EPS or Licensing Metrics mentioned Users then Qty should mentioned 12000
Note 3	The Bank may procure additional quantities, as and when required, during the contract period at the unit rates quoted by the Bidder in the Price/Rate Sheet. Where the required quantity or configuration is not explicitly covered in the Price/Rate Sheet, the additional quantity shall be procured on a pro-rata basis based on the quoted rates.
Note 4	The Bidder shall quote in the Product Licence Cost Sheet only the one-time cost applicable for the proposed licensing model, as specified below: a) **Perpetual Licensing Model:** The Product Licence Cost shall represent the complete one-time cost of the perpetual licence(s) required for the proposed solution. b) **Subscription / SaaS Model:** The Product Subscription Cost shall represent the one-time subscription cost applicable up to successful Go-Live of the solution or expiry of the initial subscription period, whichever is later. c) **Any other licensing model:** The Bidder shall clearly describe the proposed licensing model and quote the applicable one-time initial licence/subscription cost required to make the complete solution operational up to Go-Live. The Product Licence / Subscription Cost quoted in the Product Licence Cost Sheet shall include all licences, modules, components, features, users, interfaces, connectors and other mandatory licence/subscription entitlements required for implementation, testing, commissioning and successful Go-Live of the proposed solution, as applicable to the proposed licensing model.

Product License Cost					
S.No.	Solution name	License Cost Solution Description	Qty	Rate (in INR)	Total (in INR)
Note 5	The Bidder shall clearly specify the warranty period offered for the proposed solution in its technical and commercial proposal. The warranty shall commence from the date of successful Go-Live. Any delay in Go-Live attributable to the Bidder, OEM or implementation partner shall not result in any additional licence, subscription, ATS or support charges to the bank.				
Note 6	Any cost not specifically disclosed in the prescribed cost sheets but subsequently identified as mandatory for the functionality committed under this RFP shall be provided at no additional cost to the bank.				

Product Implementation cost				
S.No.	Solution Name	OEM Implementation Cost (One time) (in INR)	Bidder Implementation Support Cost (One time) (in INR)	Grand Total (Implementation Cost)
1	Security Information and Event Management (SIEM)	0	0	0
2	Security Orchestration, Automation & Response (SOAR)	0	0	0
3	User & Entity Behaviour Analytics (UEBA)	0	0	0
4	Deception Technology (Decoy/Honeypot)	0	0	0
5	Extended Detection & Response (XDR)	0	0	0
6				
7	Threat Intelligence Platform (TIP)	0	0	0
8	Vulnerability Assessment & Management (VA)	0	0	0
9	Identity Threat Detection & Response (ITDR)	0	0	0
10	Application Security Testing (AST) Tool	0	0	0
11	Cloud Security Posture Management (CSPM)	0	0	0
12	Cloud-Native Application Protection Platform (CNAPP)	0	0	0
13	Cloud Workload Protection Platform (CWPP)	0	0	0
14	Continuous Threat Exposure Management (CTEM)	0	0	0
15	Any other, please specify	0	0	0
16	Any other, please specify	0	0	0
GRAND TOTAL		0	0	0

Note 1	The Bidder shall quote the complete one-time Product Implementation Cost required for implementation, configuration, customization, integration, testing, commissioning, training and successful Go-Live of the proposed solution, as applicable.
Note 2	The quoted cost shall be comprehensive and firm and shall include all professional services, implementation resources, tools and activities required to deliver the complete solution in accordance with the requirements of the RFP.
Note 3	The Bidder shall ensure that all mandatory components, modules, interfaces, connectors, implementation activities and professional services required to achieve successful Go-Live are included in the quoted cost. No mandatory implementation cost shall be quoted separately outside this sheet.
Note 4	Any cost associated with implementation delays attributable to the Bidder, OEM or implementation partner shall be borne by the Bidder

OEM Services Cost																		
S.No.	Services Name	Description & Frequency	Services Cost Y1			Services Cost Y2			Services Cost Y3			Services Cost Y4			Services Cost Y5			Grand TOTAL Services COST (in INR)
			Quantity	Rate (In INR)	Service Cost	Quantity	Rate (In INR)	Service Cost	Quantity	Rate (In INR)	Service Cost	Quantity	Rate (In INR)	Service Cost	Quantity	Rate (In INR)	Service Cost	
	Offsite Services																	
1	Continous Red teaming services				0			0			0			0			0	0
2	Attack surface management				0			0			0			0			0	0
3	Phishing simulation				0			0			0			0			0	0
4	Dark web monitoring				0			0			0			0			0	0
5	Threat Intelligence Feed				0			0			0			0			0	0
6	Digital risk management				0			0			0			0			0	0
7	Threat Hunting services				0			0			0			0			0	0
8	Breach Attack & Simulation services				0			0			0			0			0	0
9	Security Information and Event Management (SIEM)	Architecture Assessment by Respectives solution OEMs				2		0	2		0	1		0	1		0	0
10	Security Orchestration, Automation & Response (SOAR)					2		0	2		0	1		0	1		0	0
11	User & Entity Behaviour Analytics (UEBA)					1		0	1		0	1		0	1		0	0
12	Extended Detection & Response (XDR)					1		0	1		0	1		0	1		0	0
13	Any other, please specify				0			0			0			0			0	0
14	Any other, please specify				0			0			0			0			0	0
15	Any other, please specify				0			0			0			0			0	0
	GRAND TOTAL				**0**			**0**			**0**			**0**			**0**	**0**

Notes	
Note 1	Bidder to provide the following information in the ***Description & Frequency*** column for each of the proposed product/solution for respective services: 1. Make of the Tool 2. Model of the Tool 3. Version of the proposed Tool 4. Edition 5. Frequency of the Services- Continuous/ Daily/Weekly/Monthly/Quarterly/Half-yearly/Yearly/ One time
Note 2	The bidder shall quote the service costs in alignment with the provided volumetrics and service requirements. Costs must be allocated appropriately for each respective year.Bidders should ensure that costs are distributed appropriately across the contract period
Note 3	The Bidder shall quote the OEM Offsite Services Cost for each service specified in the sheet for a period of five (5) years, i.e., Year 1 (Y1) to Year 5 (Y5).
Note 4	The quantity indicated by the Purchaser in the BOQ is the minimum required quantity/frequency for the respective service.
Note 5	The quoted rates shall be comprehensive and inclusive of all OEM professional services, resources, tools, travel, remote/offsite effort, analysis, reporting, documentation and other costs required for complete delivery of the respective service
Note 6	“Any other” items shall be used only for services that are necessary for successful operation/support of the proposed solution and are not already covered under the listed service categories. The Bidder shall clearly specify the service name, scope, frequency and pricing.

HARDWARE COST- IT INFRASTRUCTURE COST							
S.No.	Payment Milestone	Installation Cost (One time) (in INR)	IT INFRASTRUCTURE COST				Grand Total (Installation Cost + IT INFRASTRUCTURE Cost)
			Item Description/mapping with BoQ	Qty	Rate (in INR)	Total (in INR)	
DATA CENTER (PRODUCTION) - PRIMARY & HA							DC
1	Server-Compute - Configuration 1	0				0	0
2	Server-Compute - Configuration 2	0				0	0
3	Server-Compute - Configuration 3	0				0	0
4	Server-Compute - Configuration 4	0				0	0
5	Backup Server - Configuration 1	0				0	0
6	Primary Storage	0				0	0
7	Object Storage	0				0	0
8	SAN Swicthes	0				0	0
9	Long Term Storage for backup	0				0	0
10	**IT Infra Supporting Software**						
10.1	Operating System	0				0	0
10.2	Application Server Software	0				0	0
10.3	Web Server software	0				0	0
10.4	Backup Software	0				0	0
10.5	Virtualization/Containerization/HCI	0				0	0
10.6	Database	0				0	0
11	Rack	0				0	0
12	Any other, please specify	0				0	0
13	Any other, please specify	0				0	0
TOTAL DC-PRIMARY & HA		0				0	0
DISASTER RECOVERY CENTER (PRODUCTION) - PRIMARY & HA							DR
1	Server-Compute - Configuration 1	0				0	0
2	Server-Compute - Configuration 2	0				0	0
3	Server-Compute - Configuration 3	0				0	0
4	Server-Compute - Configuration 4	0				0	0
5	Backup Server - Configuration 1	0				0	0
6	Primary Storage	0				0	0
7	Object Storage	0				0	0
8	SAN Swicthes	0				0	0
9	Long Term Storage for backup	0				0	0
10	**IT Infra Supporting Software**						
10.1	Operating System	0				0	0
10.2	Application Server Software	0				0	0
10.3	Web Server software	0				0	0
10.4	Backup Software	0				0	0
10.5	Virtualization/Containerization/HCI	0				0	0
10.6	Database	0				0	0
11	Rack	0				0	0
12	Any other, please specify	0				0	0
13	Any other, please specify	0				0	0
TOTAL DR-PRIMARY		0				0	0
NON-PRODUCTION							NON-PRODUCTION
1	Server-Compute - Configuration 1	0				0	0
2	Server-Compute - Configuration 2	0				0	0
3	Server-Compute - Configuration 3	0				0	0
4	Server-Compute - Configuration 4	0				0	0
5	Backup Server - Configuration 1	0				0	0
6	Primary Storage	0				0	0
7	Object Storage	0				0	0
8	SAN Swicthes	0				0	0
9	Long Term Storage for backup	0				0	0

HARDWARE COST- IT INFRASTRUCTURE COST							
S.No.	Payment Milestone	Installation Cost (One time) (in INR)	IT INFRASTRUCTURE COST				Grand Total (Installation Cost + IT INFRASTRUCTURE Cost)
			Item Description/mapping with BoQ	Qty	Rate (in INR)	Total (in INR)	
10	**IT Infra Supporting Software**						
10.1	Operating System	0				0	0
10.2	Application Server Software	0				0	0
10.3	Web Server software	0				0	0
10.4	Backup Software	0				0	0
10.5	Virtualization/Containerization/HCI	0				0	0
10.6	Database	0				0	0
11	Rack	0				0	0
12	Any other, please specify	0				0	0
13	Any other, please specify	0				0	0
TOTAL NON-PRODUCTION		0				0	0
GRAND TOTAL		0				0	0

Notes	
Note 1	Bidder to provide the following information in the ***item Description*** column for each of the proposed product/solution for respective environment: **Hardware Item:- Server** 1. Make 2. Model 3. Number of processor per server 4. Number of cores per processor 5. RAM per server 6. HDD per server
Note 2	Bidder to provide the following information in the ***item Description*** column for each of the proposed product/solution for respective environment: **Hardware Item:- Storage (Primary)** 1. Make 2. Model 3. Number of Controllers per storage 4. Caches per controller 5. Usable Capacity (before de dupe and before compression)- RAID 6 : 6. IOPS per controller (4K - 50:50 r:w or 8K - 60:40 r:w)
Note 3	Bidder to provide the following information in the ***item Description*** column for each of the proposed product/solution for respective environment: **Hardware Item:- SAN Switch** Make Model FC Ports Throughput of each Active port and its Qty Total Ports per device Number of Diagnostic port
Note 4	Bank will provide the Ports on their LEAF and OOB switches. Bidder is required to explicitely provide the port requirements on LEAF and OOB
Note 5	Bidder to provide the following information in the ***item Description*** column for each of the proposed product/solution for respective environment: **Software Item:** 1. Make of the Solution 2. Model of the solution 3. Version of the proposed solution 4. Edition 5. Licensing Metrics
Note 5	If the proposed items have multiple configurations, the bidder is required to add additional rows to provide details of each configuration. Each row should correspond to a unique item configuration.

HARDWARE COST-APPLIANCE COST							
S.No.	Payment Milestone	Installation Cost (One time) (in INR)	APPLIANCE COST				Grand Total (Installation Cost + Hardware Cost)
			Item Description/mapping with BoQ	Qty	Rate (in INR)	Total (in INR)	
DATA CENTER (PRODUCTION) - PRIMARY + HIGH AVAILABILITY							DC
1	Security Information and Event Management (SIEM)	0				0	0
2	Security Orchestration, Automation & Response (SOAR)	0				0	0
3	User & Entity Behaviour Analytics (UEBA)	0				0	0
4	Deception Technology (Decoy/Honeypot)	0				0	0
5	Extended Detection & Response (XDR)	0				0	0
6	Network Detection & Response (NDR)						
7	Threat Intelligence Platform (TIP)	0				0	0
8	Vulnerability Assessment & Management (VA)	0				0	0
9	Identity Threat Detection & Response (ITDR)	0				0	0
10	Application Security Testing (AST) Tool	0				0	0
11	Cloud Security Posture Management (CSPM)	0				0	0
12	Cloud-Native Application Protection Platform (CNAPP)	0				0	0
13	Cloud Workload Protection Platform (CWPP)	0				0	0
14	Continuous Threat Exposure Management (CTEM)	0				0	0
15	Rack	0				0	0
16	Any other, please specify	0				0	0
17	Any other, please specify	0				0	0
TOTAL DC-PRIMARY & HA		0				0	0
DISASTER RECOVERY CENTER (PRODUCTION) - PRIMARY & HA							DR
1	Security Information and Event Management (SIEM)	0				0	0
2	Security Orchestration, Automation & Response (SOAR)	0				0	0
3	User & Entity Behaviour Analytics (UEBA)	0				0	0
4	Deception Technology (Decoy/Honeypot)	0				0	0
5	Extended Detection & Response (XDR)	0				0	0
6	Network Detection & Response (NDR)						

HARDWARE COST-APPLIANCE COST							
S.No.	Payment Milestone	Installation Cost (One time) (in INR)	APPLIANCE COST				Grand Total (Installation Cost + Hardware Cost)
			Item Description/mapping with BoQ	Qty	Rate (in INR)	Total (in INR)	
7	Threat Intelligence Platform (TIP)	0				0	0
8	Vulnerability Assessment & Management (VA)	0				0	0
9	Identity Threat Detection & Response (ITDR)	0				0	0
10	Application Security Testing (AST) Tool	0				0	0
11	Cloud Security Posture Management (CSPM)	0				0	0
12	Cloud-Native Application Protection Platform (CNAPP)	0				0	0
13	Cloud Workload Protection Platform (CWPP)	0				0	0
14	Continuous Threat Exposure Management (CTEM)	0				0	0
15	Rack	0				0	0
16	Any other, please specify	0				0	0
17	Any other, please specify	0				0	0
TOTAL DR-PRIMARY		0				0	0
NON-PRODUCTION							NON-PRODUCTION
1	Security Information and Event Management (SIEM)	0				0	0
2	Security Orchestration, Automation & Response (SOAR)	0				0	0
3	User & Entity Behaviour Analytics (UEBA)	0				0	0
4	Deception Technology (Decoy/Honeypot)	0				0	0
5	Extended Detection & Response (XDR)	0				0	0
6	Network Detection & Response (NDR)						
7	Threat Intelligence Platform (TIP)	0				0	0
8	Vulnerability Assessment & Management (VA)	0				0	0
9	Identity Threat Detection & Response (ITDR)	0				0	0
10	Application Security Testing (AST) Tool	0				0	0
11	Cloud Security Posture Management (CSPM)	0				0	0
12	Cloud-Native Application Protection Platform (CNAPP)	0				0	0
13	Cloud Workload Protection Platform (CWPP)	0				0	0

HARDWARE COST-APPLIANCE COST							
S.No.	Payment Milestone	Installation Cost (One time) (in INR)	APPLIANCE COST				Grand Total (Installation Cost + Hardware Cost)
			Item Description/mapping with BoQ	Qty	Rate (in INR)	Total (in INR)	
14	Continuous Threat Exposure Management (CTEM)	0				0	0
15	Rack	0				0	0
16	Any other, please specify	0				0	0
17	Any other, please specify	0				0	0
TOTAL NON-PRODUCTION		0				0	0
GRAND TOTAL		0				0	0
Notes							
Note 1	Bidder to provide the following information in the ***item Description*** column for each of the proposed product/solution for respective environment: **Hardware Item:- Server** 1. Make 2. Model 3. Number of processor per server 4. Number of cores per processor 5. RAM per server 6. HDD per server						
Note 2	Bidder to provide the following information in the ***item Description*** column for each of the proposed product/solution for respective environment: **Hardware Item:- Storage (Primary)** 1. Make 2. Model 3. Number of Controllers per storage 4. Caches per controller 5. Usable Capacity (before de dupe and before compression)- RAID 6 : 6. IOPS per controller (4K - 50:50 r:w or 8K - 60:40 r:w)						
Note 3	Bidder to provide the following information in the ***item Description*** column for each of the proposed product/solution for respective environment: **Hardware Item:- SAN Switch** Make Model FC Ports Throughput of each Active port and its Qty Total Ports per device Number of Diagnostic port						
Note 4	Bank will provide the Ports on their LEAF and OOB switches. Bidder is required to explicitely provide the port requirements on LEAF and OOB switches						

HARDWARE COST-APPLIANCE COST							
S.No.	**Payment Milestone**	**Installation Cost (One time) (in INR)**	**APPLIANCE COST**				**Grand Total (Installation Cost + Hardware Cost)**
			Item Description/mapping with BoQ	**Qty**	**Rate (in INR)**	**Total (in INR)**	
Note 5	Bidder to provide the following information in the ***item Description*** column for each of the proposed product/solution for respective environment: **Software Item:** 1. Make of the Solution 2. Model of the solution 3. Version of the proposed solution 4. Edition 5. Licensing Metrics						
Note 5	If the proposed items have multiple configurations, the bidder is required to add additional rows to provide details of each configuration. Each row should correspond to a unique item configuration.						

ATS/subscription Cost												
		ATS/subscription Cost										
		Y1		Y2		Y3		Y4		Y5		
S.No.	Payment Milestone	Rate (in % with respect to License Cost)	ATS/Subscriptio n Cost (in INR)	Rate (in % with respect to License Cost)	ATS/Subscrip tion Cost (in INR)	Rate (in % with respect to License Cost)	ATS/Subscr iption Cost (in INR)	Rate (in % with respect to License Cost)	ATS/Subscri ption Cost (in INR)	Rate (in % with respect to License Cost)	ATS/Subscriptio n Cost (in INR)	TOTAL ATS COST (in INR)
DATA CENTER (PRODUCTION) - PRIMARY & HA												
1	Security Information and Event Management (SIEM)											0
2	Security Orchestration, Automation & Response (SOAR)											0
3	User & Entity Behaviour Analytics (UEBA)											0
4	Deception Technology (Decoy/Honeypot)											0
5	Extended Detection & Response (XDR)											0
6												
7	Threat Intelligence Platform (TIP)											0
8	Vulnerability Assessment & Management (VA)											0
9	Identity Threat Detection & Response (ITDR)											0
10	Application Security Testing (AST) Tool											0
11	Cloud Security Posture Management (CSPM)											0
12	Cloud-Native Application Protection Platform (CNAPP)											0
13	Cloud Workload Protection Platform (CWPP)											0
14	Continuous Threat Exposure Management (CTEM)											0
15	Any other, please specify											0
16	Any other, please specify											0
GRAND TOTAL DC -PRIMARY & HA			0		0		0		0		0	0
DISASTER RECOVERY CENTER (PRODUCTION) - PRIMARY & HA												
1	Security Information and Event Management (SIEM)											0
2	Security Orchestration, Automation & Response (SOAR)											0
3	User & Entity Behaviour Analytics (UEBA)											0
4	Deception Technology (Decoy/Honeypot)											0
5	Extended Detection & Response (XDR)											0
6												
7	Threat Intelligence Platform (TIP)											0
8	Vulnerability Assessment & Management (VA)											0
9	Identity Threat Detection & Response (ITDR)											0
10	Application Security Testing (AST) Tool											0
11	Cloud Security Posture Management (CSPM)											0
12	Cloud-Native Application Protection Platform (CNAPP)											0
13	Cloud Workload Protection Platform (CWPP)											0
14	Continuous Threat Exposure Management (CTEM)											0
15	Any other, please specify											0
16	Any other, please specify											0
GRAND TOTAL DR -PRIMARY & HA			0		0		0		0		0	0
NON-PRODUCTION												
1	Security Information and Event Management (SIEM)											0
2	Security Orchestration, Automation & Response (SOAR)											0
3	User & Entity Behaviour Analytics (UEBA)											0
4	Deception Technology (Decoy/Honeypot)											0
5	Extended Detection & Response (XDR)											0
6												
7	Threat Intelligence Platform (TIP)											0
8	Vulnerability Assessment & Management (VA)											0
9	Identity Threat Detection & Response (ITDR)											0
10	Application Security Testing (AST) Tool											0
11	Cloud Security Posture Management (CSPM)											0
12	Cloud-Native Application Protection Platform (CNAPP)											0
13	Cloud Workload Protection Platform (CWPP)											0
14	Continuous Threat Exposure Management (CTEM)											0
15	Any other, please specify											0
16	Any other, please specify											0
GRAND TOTAL NON-PRODUCTION			0		0		0		0		0	0
GRAND TOTAL			0		0		0		0		0	0
Notes												

Note 1	The Bidder shall quote the Annual Technical Support (ATS) / Annual Subscription / Annual Maintenance / Renewal Cost, as applicable, for each proposed solution for a period of five (5) years, from Y1 to Y5, post Go-live of respective solution
Note 2	ATS / Annual Subscription charges shall become payable only after completion of the warranty period, wherein the warranty shall commence from the date of successful Go-Live
Note 3	The proposed solution is based on a Perpetual Licensing Model, the ATS shall be quoted separately from the one-time Product Licence Cost. The ATS shall cover the support/maintenance services specified in the RFP and shall become payable only after expiry of the warranty period.
Note 4	The proposed solution is based on a Subscription/SaaS/Term Licence Model, the Bidder shall quote the applicable annual subscription/renewal cost. Such annual subscription/renewal charges shall become payable only after expiry of the initial subscription period covered under the Produc Licence/Subscription Cost and the applicable warranty period
Note 5	Any mandatory recurring charge required for continued use, support or operation of the proposed solution after the applicable warranty/initial subscription period shall be fully disclosed and quoted in this sheet. No such charge shall be claimed separately if it has not been included in the Bidder's commercial proposal.

S.No.	Components	AMC/Hardware Subscription cost										TOTAL AMC COST (in INR)
		Y1		Y2		Y3		Y4		Y5		
		Rate (in % with respect to Hardware Cost)	AMC Cost (in INR)	Rate (in % with respect to Hardware Cost)	AMC Cost (in INR)	Rate (in % with respect to Hardware Cost)	AMC Cost (in INR)	Rate (in % with respect to Hardware Cost)	AMC Cost (in INR)	Rate (in % with respect to Hardware Cost)	AMC Cost (in INR)	
DATA CENTER (PRODUCTION) - PRIMARY & HA												DC
1	Server-Compute - Configuration 1											0
2	Server-Compute - Configuration 2											0
3	Server-Compute - Configuration 3											0
4	Server-Compute - Configuration 4											0
5	Backup Server - Configuration 1											0
6	Primary Storage											0
7	Object Storage											0
8	Long term Storage											0
9	SAN Swicthes											0
10	Tape Library											0
11	TOR Switches											0
12	OOB Switches											0
13	**IT Infra Supporting Software**											
13.1	Operating System											0
13.2	Application Server Software											0
13.3	Web Server software											0
13.4	Backup Software											0
13.5	Virtualization/Containerization/HCI											0
13.6	Database											0
14	Any other, please specify											0
15	Any other, please specify											0
16	Any other, please specify											0
	GRAND TOTAL-DC PRIMARY & HA		0		0		0		0		0	0
DR (PRODUCTION) - PRIMARY & HA												DR
1	Server-Compute - Configuration 1											0
2	Server-Compute - Configuration 2											0
3	Server-Compute - Configuration 3											0
4	Server-Compute - Configuration 4											0
5	Backup Server - Configuration 1											0
6	Primary Storage											0
7	Object Storage											0
8	Long term Storage											0
9	SAN Swicthes											0
10	Tape Library											0
11	TOR Switches											0
12	OOB Switches											0

S.No.	Components	AMC/Hardware Subscription cost										TOTAL AMC COST (in INR)
		Y1		Y2		Y3		Y4		Y5		
		Rate (in % with respect to Hardware Cost)	AMC Cost (in INR)	Rate (in % with respect to Hardware Cost)	AMC Cost (in INR)	Rate (in % with respect to Hardware Cost)	AMC Cost (in INR)	Rate (in % with respect to Hardware Cost)	AMC Cost (in INR)	Rate (in % with respect to Hardware Cost)	AMC Cost (in INR)	
13	**IT Infra Supporting Software**											
13.1	Operating System											0
13.2	Application Server Software											0
13.3	Web Server software											0
13.4	Backup Software											0
13.5	Virtualization/Containerization/HCI											0
13.6	Database											0
14	Any other, please specify											0
15	Any other, please specify											0
16	Any other, please specify											0
	GRAND TOTAL-DR PRIMARY & HA		0		0		0		0		0	0
	NON-PRODUCTION											**NON-PRODUCTION**
1	Server-Compute - Configuration 1											0
2	Server-Compute - Configuration 2											0
3	Server-Compute - Configuration 3											0
4	Server-Compute - Configuration 4											0
5	Backup Server - Configuration 1											0
6	Primary Storage											0
7	Object Storage											0
8	Long term Storage											0
9	SAN Swicthes											0
10	Tape Library											0
11	TOR Switches											0
12	OOB Switches											0
13	**IT Infra Supporting Software**											
13.1	Operating System											0
13.2	Application Server Software											0
13.3	Web Server software											0
13.4	Backup Software											0
13.5	Virtualization/Containerization/HCI											0
13.6	Database											0
14	Any other, please specify											0
15	Any other, please specify											0
16	Any other, please specify											0
	GRAND TOTAL-NON-PRODUCTION		0		0		0		0		0	0
	GRAND TOTAL		0		0		0		0		0	0

S.No.	Components	AMC/Hardware Subscription cost										TOTAL AMC COST (in INR)
		Y1		Y2		Y3		Y4		Y5		
		Rate (in % with respect to Hardware Cost)	AMC Cost (in INR)	Rate (in % with respect to Hardware Cost)	AMC Cost (in INR)	Rate (in % with respect to Hardware Cost)	AMC Cost (in INR)	Rate (in % with respect to Hardware Cost)	AMC Cost (in INR)	Rate (in % with respect to Hardware Cost)	AMC Cost (in INR)	

The Bidder shall ensure that the quoted AMC/Hardware Subscription Cost is sufficient to maintain the complete proposed infrastructure in accordance with the performance, availability, capacity, redundancy and support requirements specified in the RFP throughout the CONTRACT period.

Appliance AMC COST								
S.No.	Payment Milestone	Y1	Y2	Y3	Y4	Y5		TOTAL AMC COST (in INR)
		AMC Cost (in INR)	AMC Cost (in INR)	AMC Cost (in INR)	AMC Cost (in INR)	Rate (in % with respect to Hardware Cost)	AMC Cost (in INR)	
DATA CENTER (PRODUCTION) - PRIMARY & HA								DC-PRIMARY
1	Security Information and Event Management (SIEM)							0
2	Security Orchestration, Automation & Response (SOAR)							0
3	User & Entity Behaviour Analytics (UEBA)							0
4	Deception Technology (Decoy/Honeypot)							0
5	Extended Detection & Response (XDR)							0
6	[redacted]							0
7	Threat Intelligence Platform (TIP)							0
8	Vulnerability Assessment & Management (VA)							0
9	Identity Threat Detection & Response (ITDR)							0
10	Application Security Testing (AST) Tool							0
11	Cloud Security Posture Management (CSPM)							0
12	Cloud-Native Application Protection Platform (CNAPP)							0
13	Cloud Workload Protection Platform (CWPP)							0
14	Continuous Threat Exposure Management (CTEM)							0
15	Any other, please specify							0
16	Any other, please specify							0
	GRAND TOTAL-DC PRIMARY & HA						0	0
DR (PRODUCTION) - PRIMARY & HA								DR-PRIMARY
1	Security Information and Event Management (SIEM)							0
2	Security Orchestration, Automation & Response (SOAR)							0
3	User & Entity Behaviour Analytics (UEBA)							0
4	Deception Technology (Decoy/Honeypot)							0
5	Extended Detection & Response (XDR)							0
6	[redacted]							0
7	Threat Intelligence Platform (TIP)							0
8	Vulnerability Assessment & Management (VA)							0
9	Identity Threat Detection & Response (ITDR)							0
10	Application Security Testing (AST) Tool							0
11	Cloud Security Posture Management (CSPM)							0
12	Cloud-Native Application Protection Platform (CNAPP)							0
13	Cloud Workload Protection Platform (CWPP)							0
14	Continuous Threat Exposure Management (CTEM)							0
15	Any other, please specify							0
16	Any other, please specify							0
	GRAND TOTAL-DR PRIMARY & HA						0	0
NON-PRODUCTION								NON-PRODUCTION
1	Security Information and Event Management (SIEM)							0
2	Security Orchestration, Automation & Response (SOAR)							0
3	User & Entity Behaviour Analytics (UEBA)							0
4	Deception Technology (Decoy/Honeypot)							0
5	Extended Detection & Response (XDR)							0
6	[redacted]							0
7	Threat Intelligence Platform (TIP)							0
8	Vulnerability Assessment & Management (VA)							0
9	Identity Threat Detection & Response (ITDR)							0
10	Application Security Testing (AST) Tool							0
11	Cloud Security Posture Management (CSPM)							0
12	Cloud-Native Application Protection Platform (CNAPP)							0
13	Cloud Workload Protection Platform (CWPP)							0
14	Continuous Threat Exposure Management (CTEM)							0
15	Any other, please specify							0
16	Any other, please specify							0
	GRAND TOTAL-NON-PRODUCTION						0	0
	GRAND TOTAL						0	0
NOTE	The Bidder shall ensure that the quoted AMC/Hardware Subscription Cost is sufficient to maintain the complete proposed infrastructure in accordance with the performance, availability, capacity, redundancy and support requirements specified in the RFP throughout the CONTRACT period.							

FM/ O&M Cost																
S.No.	Profile	Y1			Y2			Y3			Y4			Y5			TOTAL FM COST
		Total Resources (A1)	Rate per resource (B1)	Total Cost (A1xB1)	Total Resources (A2)	Rate per resource (B2)	Total Cost (A2xB2)	Total Resources (A3)	Rate per resource (B3)	Total Cost (A3xB3)	Total Resources (A4)	Rate per resource (B4)	Total Cost (A4 x B4)	Total Resources (A5)	Rate per resource (B5)	Total Cost (A5xB5)	
1	Project Manager-Operations			0			0			0			0			0	0
2	L1			0			0			0			0			0	0
3	L2			0			0			0			0			0	0
4	L3			0			0			0			0			0	0
5	Any other, please specify			0			0			0			0			0	0
6	Any other, please specify			0			0			0			0			0	0
7	Any other, please specify			0			0			0			0			0	0
8	Any other, please specify			0			0			0			0			0	0
GRAND TOTAL				**0**			**0**			**0**			**0**			**0**	**0**
Note																	
1	The Bidder shall quote the complete Facility Management / Operations & Maintenance (FM/O&M) manpower cost for a period of five (5) years, from Y1 to Y5.																
2	Where OEM-specific technical expertise is required, the Bidder shall ensure that appropriately OEM-certified/qualified resources are deployed for the relevant technology, as specified in the RFP.																
3	The number of resources quoted for each year shall represent the total resources required to meet the specified service levels, including resources required for shifts, leave, weekly offs, holidays, training, backup and other planned/unplanned absences, wherever applicable.																
4	The Bidder shall ensure continuity of services throughout the contract period. Any absence, resignation, attrition or replacement of deployed personnel shall not affect the required service levels.																
5	24×7 or shift-based operations are specified in the RFP, the Bidder shall factor the complete manpower requirement for all shifts into the quoted resource count and rates.																
6	The Bidder shall be fully responsible for ensuring that the resources quoted are sufficient to meet all operational, monitoring, incident management, problem management, change management, reporting, maintenance and SLA requirements specified in the RFP.																

Other Cost																					
S.No.	Item	Description	Implementation			Y1			Y2			Y3			Y4			Y5			GRAND TOTAL
			Qty	Rate	Total	Qty	Rate	Total	Qty	Rate	Total	Qty	Rate	Total	Qty	Rate	Total	Qty	Rate	Total	
1	Customization/CR Cost	Unit = person day				100		0													
2	Any other please specify																				
3	Any other please specify																				
GRAND TOTAL								0													0
Note:																					
1	Customization/CR Cost- The rate per person day is to be provided for any additional items/ Change sought by bank over and above the defined scope & terms during the contract																				
2	The Bidder shall mandatorily quote the Customization / Change Request (CR) Cost in the prescribed commercial sheet.																				
3	The quoted rate shall be all-inclusive of the professional effort required for customization/CR, including analysis, design, development/configuration, testing, documentation, deployment and associated technical effort																				
4	The 100 Person-Days indicated in the commercial sheet shall be considered for commercial evaluation purposes. Actual utilization of Person-Days, if required, shall be based on approved Change Requests issued by the bank during the contract period and shall be governed by the applicable terms of the RFP/Contract.																				
5	The Rate per Person-Day shall remain firm, fixed and unchanged for the entire duration of the Contract, irrespective of the year in which the Customization/CR activity is undertaken.																				
6	The quoted rate shall be applicable for each Person-Day utilized for approved Customization/CR activities, irrespective of the resource level/profile deployed for such activity																				

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1	55–56	7.4.3 Attack surface management	7.4.3	The Bidder shall provide continuous discovery, monitoring, classification, and risk assessment of the Bank's external and internal attack surface. Discovery of internet-facing and internal assets.	Considering that the ASM Managed Service covers both the Bank's external and internal attack surfaces, please confirm that complementary OEM technologies/tools may be utilized, as required, for delivery of the respective external and internal attack-surface requirements, while collectively meeting all stated requirements of the ASM Managed Service for the Bank's external and internal attack surface.	Please refer Addendum for revised clause
2	56	7.4.3 Attack surface management	7.4.3	Discovery of internet-facing and internal assets. Identification of exposed services, applications, APIs, domains, cloud assets, certificates, and digital infrastructure.	Please confirm that discovery of the internal attack surface shall include maintaining a consolidated inventory of internal cyber assets by aggregating and correlating available asset and configuration information across supported on-premises, cloud, identity, endpoint, network and security environments.	Please refer Addendum for revised clause
3	56	7.4.3 Attack surface management	7.4.3	Continuous exposure monitoring. Identification of misconfigurations and security exposures.	Please confirm that internal attack-surface monitoring shall include current and historical asset/configuration visibility and identification of relevant configuration changes, deviations and drift, including visibility of the previous and current configuration state, what changed and when.	No Change, Please be guided by the RFP. Bank is looking for external attack surface management
4	56	7.4.3 Attack surface management	7.4.3	Continuous exposure monitoring. Risk prioritization based on business impact.	Please confirm that internal attack-surface monitoring shall support predefined and Bank-defined metrics, monitoring criteria, thresholds and compliance-relevant conditions/rules for relevant asset, configuration, security and operational attributes, including conditions aligned to applicable Bank-defined security standards, policies and configuration baselines, with configurable change detections, alerts and reporting for identified deviations.	No Change, Please be guided by the RFP. Bank is looking for external attack surface management
5	55–56	7.4.3 Attack surface management	7.4.3	The Bidder shall provide continuous discovery, monitoring, classification, and risk assessment of the Bank's external and internal attack surface. Continuous exposure monitoring.	Please confirm that internal attack-surface monitoring shall maintain time-stamped historical asset, configuration and change information for at least 12 months, with facility to review historical states and changes for investigation, audit readiness, control validation and compliance-assurance purposes.	No Change, Please be guided by the RFP. Bank is looking for external attack surface management
6	56	7.4.3 Attack surface management	7.4.3	Discovery of internet-facing and internal assets. Identification of exposed services, applications, APIs, domains, cloud assets, certificates, and digital infrastructure.	Please confirm that internal attack-surface visibility shall include supported network and network-security assets and relevant available configuration information, including device, interface, VLAN, firewall, NAT, VPN and certificate information, where available and applicable to the respective supported technology, for identifying relevant configuration deviations and security exposures.	Please refer Addendum for revised clause
7	56	7.4.3 Attack surface management	7.4.3	Identification of misconfigurations and security exposures. Recommendations for attack surface reduction.	Please confirm that identified internal configuration/exposure conditions may be re-evaluated following remediation during a subsequent applicable assessment/data-collection cycle, to validate whether the identified condition continues to exist.	No Change, Please be guided by the RFP. Bank is looking for external attack surface management
8	32	7.2.2 Services	7.2.2	Attack Surface Management (ASM) — Managed Service; Continuous / 24×7 monitoring; Weekly discovery/update; Monthly reporting.	Please confirm that the internal attack-surface capability shall provide centralized search, filtering, dashboards, visualizations and reports across relevant asset, identity, configuration, change and available security/risk information, with facility to export relevant information/evidence for use in the ASM Managed Service's prescribed weekly discovery/update and monthly reporting cycle.	No Change, Please be guided by the RFP
9	32	7.2.2 Services	7.2.2	Attack Surface Management (ASM) — Managed Service; Continuous / 24×7 monitoring; Weekly discovery/update; Monthly reporting.	Please confirm that one or more complementary OEM technologies/tools may be utilized for delivery of the complete ASM Managed Service, providing the respective external and internal attack-surface requirements, while collectively meeting all applicable ASM Managed Service requirements.	No Change, Please be guided by the RFP
10	102, 120–123	Eligibility Criteria	Eligibility Criteria / OEM Requirements	MAF should also be submitted from the following services OEMs: 3. Attack Surface management	Where complementary OEM technologies/tools are utilized for delivery of the complete ASM Managed Service, please confirm that separate MAFs are required to be submitted by the respective OEMs for the external and internal attack-surface management services requirements.	No Change, Please be guided by the RFP
11	54–55	7.4 Functional Requirement - Services (Offsite Services)	7.4	The Bidder shall ensure compliance with all applicable Government of India guidelines, RBI directives, CERT-In advisories, regulatory requirements, and the Bank's policies relating to data localization, data privacy, data sharing, and information security. All tools/platforms proposed for delivery of these services shall comply with the Bank's applicable information security, data protection, access control, logging, audit, and regulatory requirements.	With reference to the data-localization requirements applicable to Offsite Managed Services, including hosting of the Managed Service platform within India, please confirm that the Bank's target systems/data sources configured for inspection and the permitted destinations/integrations for collected data shall also be located in India.	Bank's DC and DR are located in India. Further Detail shall be shared with the successful
12	56, 257	7.4.3 / 16.21.1 Current IT assets	7.4.3 / 16.21.1	Discovery of internet-facing and internal assets. Servers deployed with OS, DB, Web/app component, middleware's, agents and other applications / software, private & public cloud setups, emerging technologies etc. – 2500; Database – 300; Intranet and internet facing business & non-business applications like CBS, Internet Banking, Mobile Banking, HRMS, O365 etc. – 200; Desktops with various agents like AV, DLP, NAC, ITAM etc. – 12000; Routers & Switches – 7200. Note: The count of IT & Security Infra as listed above is tentative.	Considering the requirement for discovery of internal assets to provide continuous discovery, monitoring, classification, and risk assessment of the Bank's internal attack surface under the ASM Managed Service, please clarify the applicable quantities of servers and desktops to be considered for sizing and licensing, currently indicated in the RFP as 2,500 servers and 12,000 desktops during the contract period.	Bank is lookig for External Attack Surface management, that have been exposed to public
13	258, 260	16.21.2 Volumetrics-Solution-wise Requirements	16.21.2	XDR (Extended Detection and Response) solution for 12,000 users scalable to 14000 Users' endpoint 12000 scalable to 16000	Considering the user volumetrics specified for XDR and ITDR, please clarify whether 12,000 users, as currently indicated in the RFP, shall be considered for sizing and licensing of the discovery, inventory and monitoring of the Bank's internal attack surface under the ASM Managed Service, including the required scalability during the contract period.	Please refer addendum for revised Volumetrics

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
14	55–56	7.4.3 Attack surface management	7.4.3	The Bidder shall provide continuous discovery, monitoring, classification, and risk assessment of the Bank's external and internal attack surface. Discovery of internet-facing and internal assets.	Considering that the ASM Managed Service covers both the Bank's external and internal attack surfaces, please confirm that complementary OEM technologies/tools may be utilized, as required, for delivery of the respective external and internal attack-surface requirements, while collectively meeting all stated requirements of the ASM Managed Service for the Bank's external and internal attack surface.	Please refer Addendum for revised clause
15	56	7.4.3 Attack surface management	7.4.3	Discovery of internet-facing and internal assets. Identification of exposed services, applications, APIs, domains, cloud assets, certificates, and digital infrastructure.	Please confirm that discovery of the internal attack surface shall include maintaining a consolidated inventory of internal cyber assets by aggregating and correlating available asset and configuration information across supported on-premises, cloud, identity, endpoint, network and security environments.	Please refer Addendum for revised clause
16	56	7.4.3 Attack surface management	7.4.3	Continuous exposure monitoring. Identification of misconfigurations and security exposures.	Please confirm that internal attack-surface monitoring shall include current and historical asset/configuration visibility and identification of relevant configuration changes, deviations and drift, including visibility of the previous and current configuration state, what changed and when.	No Change, Please be guided by the RFP. Bank is looking for external attack surface management
17	56	7.4.3 Attack surface management	7.4.3	Continuous exposure monitoring. Risk prioritization based on business impact.	Please confirm that internal attack-surface monitoring shall support predefined and Bank-defined metrics, monitoring criteria, thresholds and compliance-relevant conditions/rules for relevant asset, configuration, security and operational attributes, including conditions aligned to applicable Bank-defined security standards, policies and configuration baselines, with configurable change detections, alerts and reporting for identified deviations.	No Change, Please be guided by the RFP. Bank is looking for external attack surface management
18	55–56	7.4.3 Attack surface management	7.4.3	The Bidder shall provide continuous discovery, monitoring, classification, and risk assessment of the Bank's external and internal attack surface. Continuous exposure monitoring.	Please confirm that internal attack-surface monitoring shall maintain time-stamped historical asset, configuration and change information for at least 12 months, with facility to review historical states and changes for investigation, audit readiness, control validation and compliance-assurance purposes.	No Change, Please be guided by the RFP. Bank is looking for external attack surface management
19	56	7.4.3 Attack surface management	7.4.3	Discovery of internet-facing and internal assets. Identification of exposed services, applications, APIs, domains, cloud assets, certificates, and digital infrastructure.	Please confirm that internal attack-surface visibility shall include supported network and network-security assets and relevant available configuration information, including device, interface, VLAN, firewall, NAT, VPN and certificate information, where available and applicable to the respective supported technology, for identifying relevant configuration deviations and security exposures.	Please refer Addendum for revised clause
20	56	7.4.3 Attack surface management	7.4.3	Identification of misconfigurations and security exposures. Recommendations for attack surface reduction.	Please confirm that identified internal configuration/exposure conditions may be re-evaluated following remediation during a subsequent applicable assessment/data-collection cycle, to validate whether the identified condition continues to exist.	No Change, Please be guided by the RFP. Bank is looking for external attack surface management
21	32	7.2.2 Services	7.2.2	Attack Surface Management (ASM) — Managed Service; Continuous / 24×7 monitoring; Weekly discovery/update; Monthly reporting.	Please confirm that the internal attack-surface capability shall provide centralized search, filtering, dashboards, visualizations and reports across relevant asset, identity, configuration, change and available security/risk information, with facility to export relevant information/evidence for use in the ASM Managed Service's prescribed weekly discovery/update and monthly reporting cycle.	No Change, Please be guided by the RFP
22	32	7.2.2 Services	7.2.2	Attack Surface Management (ASM) — Managed Service; Continuous / 24×7 monitoring; Weekly discovery/update; Monthly reporting.	Please confirm that one or more complementary OEM technologies/tools may be utilized for delivery of the complete ASM Managed Service, providing the respective external and internal attack-surface requirements, while collectively meeting all applicable ASM Managed Service requirements.	No Change, Please be guided by the RFP
23	102, 120–123	Eligibility Criteria	Eligibility Criteria / OEM Requirements	MAF should also be submitted from the following services OEMs: 3. Attack Surface management	Where complementary OEM technologies/tools are utilized for delivery of the complete ASM Managed Service, please confirm that separate MAFs are required to be submitted by the respective OEMs for the external and internal attack-surface management services requirements.	No Change, Please be guided by the RFP
24	54–55	7.4 Functional Requirement - Services (Offsite Services)	7.4	The Bidder shall ensure compliance with all applicable Government of India guidelines, RBI directives, CERT-In advisories, regulatory requirements, and the Bank's policies relating to data localization, data privacy, data sharing, and information security. All tools/platforms proposed for delivery of these services shall comply with the Bank's applicable information security, data protection, access control, logging, audit, and regulatory requirements.	With reference to the data-localization requirements applicable to Offsite Managed Services, including hosting of the Managed Service platform within India, please confirm that the Bank's target systems/data sources configured for inspection and the permitted destinations/integrations for collected data shall also be located in India.	Bank's DC and DR are located in India. Further Detail shall be shared with the successful
25	56, 257	7.4.3 / 16.21.1 Current IT assets	7.4.3 / 16.21.1	Discovery of internet-facing and internal assets. Servers deployed with OS, DB, Web/app component, middleware's, agents and other applications / software, private & public cloud setups, emerging technologies etc. – 2500; Database – 300; Intranet and internet facing business & non-business applications like CBS, Internet Banking, Mobile Banking, HRMS, O365 etc. – 200; Desktops with various agents like AV, DLP, NAC, ITAM etc. – 12000; Routers & Switches – 7200. Note: The count of IT & Security Infra as listed above is tentative.	Considering the requirement for discovery of internal assets to provide continuous discovery, monitoring, classification, and risk assessment of the Bank's internal attack surface under the ASM Managed Service, please clarify the applicable quantities of servers and desktops to be considered for sizing and licensing, currently indicated in the RFP as 2,500 servers and 12,000 desktops during the contract period.	Bank is lookig for External Attack Surface management, that have been exposed to public
26	258, 260	16.21.2 Volumetrics-Solution-wise Requirements	16.21.2	XDR (Extended Detection and Response) solution for 12,000 users scalable to 14000 Users' endpoint 12000 scalable to 16000	Considering the user volumetrics specified for XDR and ITDR, please clarify whether 12,000 users, as currently indicated in the RFP, shall be considered for sizing and licensing of the discovery, inventory and monitoring of the Bank's internal attack surface under the ASM Managed Service, including the required scalability during the contract period.	Please refer addendum for revised Volumetrics

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
27		PSB_Functional & Technical Compliance	Application Security - Functional Specification - SAST	Pt 3 - To enable the virtual segregation of various data types, the proposed solution should support an unlimited number of virtual storage groups or indexes. Each index or virtual storage group should be designated for searching specific data, with a configurable retention period tailored to each index.	This is not applicable in case of application security testing. Request bnak to remove the clause	Clause is not refering to this RFP
28		PSB_Functional & Technical Compliance	Application Security - Functional Specification - DAST	Pt 92 - The solution must be capable to generate report in following format: 5. Code snippets.	In case of DAST, there are no source codes, so code snippets are not possible. Kindly remove the code snippet.	Clause is not refering to this RFP
29		RFP - 7. Scope of Work	7.3.1.9 Application security testing Tool: Features & modules:	7. Integration of IT Security Solution with SOC Capabilities Including AI, ML, and Automation. The SOC Platform should be full integrable with organisation's IT security solution. This integration shall: a) Support Bi-directional Data Exchange: Enable seamless, real-time exchange of threat intelligence, alerts, logs, and incident data between the IT security solution and the SOC systems (e.g., SIEM, SOAR). b) Enable Automated Response Workflows: Integrate with SOC automation tools (e.g., SOAR platforms) to: i Trigger automated incident response actions based on predefined playbooks. ii Support auto-remediation, quarantine, or escalation steps based on severity levels. iii Provide audit trails for automated decisions and actions c) Ensure Interoperability and Extensibility: Support open standards and APIs (e.g., STIX/TAXII, REST APIs) to ensure compatibility with current and future SOC tools and frameworks d) Maintain Security and Compliance: All data exchanged between the IT security solution and SOC must be encrypted in transit and at rest, and comply with relevant regulatory standards (e.g., ISO 27001, NIST, GDPR).	This paragraph is mentioned in general under scope of work across all the products/technologies in the RFP, however it would not be applicable in case of application security technology as AST in general works at pre-production/development stage only. Request bank to remove this clause.	Clause is not refering to this RFP
30		RFP - 7. Scope of Work	7.3.1.9 Application security testing Tool: Bidder/OEM Responsibility:	4. Integrate the solution with all the IT sources (Bank's existing & new applications, IT Infrastructures, network & Security infrastructures, Endpoints (if required by bank) etc.)	This clause is mentioned in general under scope of work across many products / technologies in the RFP, however it would not be applicable in case of application security technology as AST in general integrates with applications only for CI/CD integrations. Request bank to remove this clause.	Clause is not refering to this RFP
31		RFP - 15.21 Annexure 21: Sizing/Volumetrics	9. Application Security Testing Tool	HA (Active/Active – N+N redundant Deployment) at DC and HA (Active/Active – N+N redundant Deployment) at DR	Application Security Testing in general works at pre-production/development stage only, HA is not mandatory or required individually at DC & DR. As putting HA at both DC & DR will unncesarily shoot up the HW cost. However if bank feels to implement HA, same can be provisioned between DC & DR. Reqeust bank to modify the clause.	Clause is not refering to this RFP
32		RFP - 15.21 Annexure 21: Sizing/Volumetrics	9. Application Security Testing Tool	All the inline components of the solution must operate in high availability mode. In the event of any component failure, the system should automatically initiate failovers within seconds, ensuring uninterrupted functionality without requiring manual intervention.	Application Security Testing as a technology in general works at developemnt/pre-production/UAT stage only. And as a solution these are not placed inline in production environment (live), hence there is no concept of active-active automatic failover between DC-DR at the solution level. But the same can be achieved at the network/server level using load balancers avaialble or through defined manual SOPs over in bank's environment. Request bank to modify the clause accordingly.	No Change, Please be guided by the RFP. The bidder must design the solution to fully comply with the RFP requirements, ensuring that in case of a failover, the system meets the defined SLA for availability, RTO, and RPO. The bidder is required to adhere to the deployment requirements outlined in the RFP when designing and proposing the solution architecture.
33		RFP - 15.21 Annexure 21: Sizing/Volumetrics	9. Application Security Testing Tool	DAST - 1 Enterprise license (Number of applications (WEB Facing) with at least 25 application	Bank has asked for unlimited number of application in case of SAST, however in case of DAST, only 25 applications count is menitoned. As DAST specs has a meniton of mobile and API scanning as well, request bank to confirm the specific count for web, mobile and APIs which needs to be scanned via DAST ?	No Change, Please be guided by the RFP
34		PSB_Functional & Technical Compliance	SIEM & DATA LAKE - Functional Specification	Pt 3 - To enable the virtual segregation of various data types, the proposed solution should support an unlimited number of virtual storage groups or indexes. Each index or virtual storage group should be designated for searching specific data, with a configurable retention period tailored to each index	This clause is a proprietary feature, favouring a single OEM. Request bank to delete the clause for wider participation.	Clause is not refering to this RFP
35		PSB_Functional & Technical Compliance	SIEM & DATA LAKE - Functional Specification	Pt 6 - The proposed solution should be able to receive, ingest and index structured or unstructured data without schema or normalization and no events should be dropped. if log source changes the format of log data. Unparsed events should be usable for corelation and machine learning models.	This clause is a proprietary feature, favouring a single OEM. Request bank to delete the clause for wider participation.	Clause is not refering to this RFP
36		PSB_Functional & Technical Compliance	SIEM & DATA LAKE - Functional Specification	Pt 8 - The solution must ensure that if data ingested is not parsed then with the new parser old data ingested should also be parsed without need to re-ingest data throughout the retention period of online 180 days and 365 days of archival. Use Case: Referencing old data for predictive analytics, proactive monitoring etc. By not reindexing and re-ingesting securityanalyst would save storage cost and identify and pin point attack intime.	This clause is a proprietary feature, favouring a single OEM. Request bank to delete the clause for wider participation.	Clause is not refering to this RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
37		PSB_Functional & Technical Compliance	SIEM & DATA LAKE - Functional Specification	Pt 86 - The solution must support viewing data in different formats or schemas without re-ingesting, re-indexing, redundant storage. Historical data also should be viewed as per new format or schema without re-ingesting or without additional storage utilization. Indicative Use Case: Referencing old data for predictive analytics, proactive monitoring etc. By not reindexing and re- ingesting security analyst would save storage cost and identify and pinpoint attack in time.	This clause is a proprietary feature, favouring a single OEM. Request bank to delete the clause for wider participation.	Clause is not refering to this RFP
38		PSB_Functional & Technical Compliance	SIEM & DATA LAKE - Functional Specification	Pt 89 - Old data should be parsed with new parser without re-ingesting or re-indexing the data.	This clause is a proprietary feature, favouring a single OEM. Request bank to delete the clause for wider participation.	Clause is not refering to this RFP
39		PSB_Functional & Technical Compliance	SIEM & DATA LAKE - Functional Specification - SBDL	Pt 142 - Conversational Interface with Agentic AI Support enabling SOC analysts to interact with SOC-Blg Data data via natural language, receive AI-suggested remediations, and trigger autonomous actions within workflows.Real-time Semantic Retrieval Pipeline to enable intelligent alert investigation and knowledge access within SOC-Blg Data	This clause is a proprietary feature, favouring a single OEM. Request bank to delete the clause for wider participation.	Clause is not refering to this RFP
40		PSB_Functional & Technical Compliance	SIEM & DATA LAKE - Functional Specification - SBDL	Pt 143 - The system shall provide advanced threat detection capabilities through keyword and semantic search, augment SOC-Big Data Lake using NLP and machine learning for contextual analysis and prioritization, integrate with high-performance vector databases for real-time semantic retrieval, and support modular AI components such as embedding generation to process heterogeneous log and alert data formats.	This clause is a proprietary feature, favouring a single OEM. Request bank to delete the clause for wider participation.	Clause is not refering to this RFP
41		PSB_Functional & Technical Compliance	SIEM & DATA LAKE - Functional Specification - SBDL	Pt 145 - The solution should offer the ease of creating custom playbooks which needs to be flexible and multi-conditional.	This is a SOAR capability, we request bank should be moved under SOAR clauses.	Clause is not refering to this RFP
42		PSB_Functional & Technical Compliance	UEBA - Functional Specification - SBDL	Pt 31 - UEBA should perform identity resolution to find the real-time association between endpoints, IP addresses, host names, endpoint location, and users, and maintain these associations over time	This clause is a proprietary feature, favouring a single OEM. Request bank to delete the clause for wider participation.	Clause is not refering to this RFP
43		RFP - 7. Scope of Work	7.12 Other In-Scope Services: 7.12.2 Escrow	The Bank and the Bidder shall agree to appoint an escrow agent to provide escrow mechanism for the deposit of the source code of any customization done on Commercial off the shelf software products supplied/ procured by the Bidder to the Bank in order to protect its interests in an eventual situation. The Bank and the Bidder shall enter into a tripartite escrow agreement with the designated escrow agent, which will set out, inter alia, the events of the release of the source code and the obligations of the escrow agent. Costs for the Escrow will be borne by the Bidder.	Source code is OEM's Intellectual Property (IP), we request bank to delete this clause.	Clause is not refering to this RFP
44		RFP - 15.21 Annexure 21: Sizing/Volumetrics	1. SIEM 2. SOC Big Data Lake (Bank's DC and DR each) 3. SOAR 5. UEBA	1. Logs (Normalized Logs & Data) should be stored for 6 months on primary storage (SSD/NVME) and 9 months on object storage. 2. Logs should be stored for 3 months on primary storage (SSD/NVME) and 18 months on object storage at on-premises storage. 3. Logs should be stored for 6 months on primary storage (SSD/NVME) 5. Logs should be stored for 6 months on primary storage (SSD/NVME)	Bank has asked for dedicated S-BDL solution which is used as a common data lake/repository for all NGSOC solution components. However here, this seems to be little contradictory as bank has asked different retention period as primary storage for different components and again different retention period (for object storage) for different components. We suggest bank to ask for single retention storage policy for both primary and object storage for all the integrated solutions with SBDL common data repository.	Clause is not refering to this RFP
45		8	Contract Period	The bank may, at its sole discretion, extend the contract for an additional period of two years, in one-year increments tranches. During the extension period, the annual rates of respective support components shall not exceed 15-20% of the last year's support components (ATS/ AMC/ O&M/ Subscription/ Services) prices.	It is requested that the annual rates of the support components shall be negotiated and agreed upon mutually.	No Change, Please be guided by the RFP
46		13.1	Assignment & Subcontracting	The selected bidder shall not subcontract or permit anyone to perform any of the work, service or other performance required under the contract.	We request that subcontracting be allowed given the scope of services.	No Change, Please be guided by the RFP
47		13.2	Delays in the Bidder's Performance	The bidder must strictly adhere to the schedule, as specified in the purchase contract/purchase order, executed between the Parties for performance of the obligations, arising out of the purchase contract and any delay in completion of the obligations by the Bidder will enable Bank to resort to any or both of the following: a. Claiming Liquidated Damages b. Termination of the purchase agreement fully or partly and claim liquidated damages. c. Execution of Bid Declaration Form / Invoking EMD or Performance Bank Guarantee	We request that a notice cum cure period of atleast 30 days be provided to the bidder to rectify any breach/delay.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
48		13.4	Dispute Resolution	If any dispute, difference or claim arises between the parties hereto in connection with the validity, interpretation, implementation or alleged breach of the terms of this Agreement or anything done or omitted to be done pursuant to this Agreement, the Parties shall attempt in the first instance to resolve the same through negotiation. If the dispute is not resolved through negotiation within 30 (thirty) days after commencement of discussions, then, the parties shall be at liberty to approach competent court of law at Delhi for adjudication of the disputes.	We request that the any dispute arising between the parties under the RFP/agreement be referred to arbitration, and the arbitration proceedings be conducted in accordance with the Arbitration and Conciliation Act,1996 and the Rules thereunder (as amended from time to time). Further, the arbitration be conducted by a sole arbitrator to be appointed mutually by the Parties. The seat and venue of arbitration be New Delhi, and the arbitral proceedings be conducted in English. We request changes in the clause to indicate the above.	No Change, Please be guided by the RFP
49		13.15	Order Cancellation	The Bank reserves the right to cancel the contract placed on the selected bidder and recover the expenditure incurred by the Bank on the following circumstances: a) Non submission of acceptance of order within 7 days of order. b) Excessive delay in execution of orders placed by the Bank. c) The selected bidder commits a breach of any of the terms and conditions of the bid. d) The bidder goes into liquidation voluntarily or otherwise. e) An attachment is levied or continues to be levied for a period of 7 days upon the effects of the bid. f) The progress made by the selected bidder is found to be unsatisfactory. g) If deductions on account of liquidated Damages/penalties exceeds more than 10% of the total contract price. h) If found blacklisted by any Govt. Department / PSU / other Banks / CERT-In, during contracted period. i) Non satisfactory performance of the Project in terms of affecting the Core Systems of the Bank or the Core Business of the Bank and the functioning of the Branches/Offices of the Bank.	1. Please clarify what you mean by "recovering expenditure"? 2. We request that a notice cum cure period of atleast 30 days be provided to the bidder in the event of termination for any default.	Clause is not refering to this RFP
50		13.15	Order Cancellation	Bank shall serve the notice of termination to the bidder at least 30 days prior of its intention to terminate services without assigning any reasons.	We request that a period of atleast 90 days be given before termination of the contract for convenience. Also, please confirm that PSB shall additionally pay to the Bidder for all work done till the date of termination, as well as for the orders already placed with OEMs/Licensors, which orders cannot be cancelled with the OEMs/Licensors, cancellation costs, if any, levied by the OEMs/Licensors, and logistical and administrative expenses, if any, incurred by the Bidder on account of such cancellations, which expenses shall be billed on actuals. Further, if the Bidder is providing any products/goods on opex or lease model, then PSB shall pay the Bidder the residual value of the products.	No Change, Please be guided by the RFP
51		13.15	Order Cancellation	The Bank reserves the right to recover any dues payable by the selected bidder from any outstanding amount to the credit of the selected bidder, including the pending bills and security deposit, if any, under this contract.	We request that any dues paayble only be recovered/adjusted with any liquidated damages or penalties levied against the bidder, and not against any other amount payable to the bidder for the services rendered.	No Change, Please be guided by the RFP
52					We request that the following clause on non-solicitation be added in the contract: "During the term of the contract and for a period of one (1) year following its termination, the Bank shall not directly or indirectly, either through itself or through any of its service providers or vendors, solicit or engage in any capacity, any personnel or employee or resources of the bidder, engaged in rendering any services or deployed at the Bank'a location. However, this will not apply to personnel who independently respond to general job opening postings (such as general newspaper advertisements, employment agency referrals and internet postings etc.) not directly targeting such personnel/employee.	Clause is not refering to this RFP
53		7.3.1.7	Features and Modules: 2(b)	Enable Automated Response Workflows: Integrate with SOC automation tools (e.g., SOAR platforms) to: i Trigger automated incident response actions based on predefined playbooks. ii Support auto-remediation, quarantine, or escalation steps based on severity levels. iii Provide audit trails for automated decisions and actions	We don't directly trigger automated incident response actions, but we enable them by feeding enriched threat intelligence into SIEM, SOAR, and SOC tools. This ensures those systems can immediately execute playbooks, auto-remediation, quarantine, or escalation based on severity, while also maintaining audit trails of all actions taken. But If the ask is to enable automated response by integrating with SIEM/SOAR, that is possible	Clause is not refering to this RFP
54		7.3.1.7	Bidder/OEM Responsibility: 3rd point	The bank will implement its security solutions—such as agents, dedicated instances, and tools like HIPS, RASP, WAF, DAM, and third-party firewalls—on a dedicated instance specifically provisioned for the bank.	This requirement is out of scope for DRP/ASM products. Such controls typically fall under cloud or infrastructure security solutions (e.g., AWS, GCP, Azure) and should therefore be removed from DRP/ASM requirements.	Clause is not refering to this RFP
55		7.3.1.7	Bidder/OEM Responsibility: 4th Point	The Virtual Private Cloud (VPC) in the cloud environment must be configured to align with the bank's on-premises/cloud security policies and controls, ensuring consistent enforcement of security standards across both infrastructures	This requirement pertains to cloud infrastructure security and posture management and has no direct relation to DRP/ASM solutions, which are focused on external threat intelligence, digital risk protection, and attack surface monitoring. We kindly request to either justify its relevance to DRP/ASM or remove it from the DRP/ASM scope	Clause is not refering to this RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
56		7.3.2.5	Point 8	Monitoring spam traps to detect phishing mails.	Spam trap monitoring is generally an email security function and not part of DRP/ASM. CloudSEK does not operate spam traps; instead, we address phishing risks through proactive monitoring of domains, apps, dark web sources, credential leaks, and takedowns. Could you please clarify the intended use case for including spam trap monitoring under DRP/ASM? Based on that, we can suggest the best-fit alternative or request removal of this requirement from the DRP/ASM scope.	Clause is not refering to this RFP
57		7.3.2.5	Point 13	Inject fake credentials into the phishing portals and fraudulent apps and provide details to the Bank for monitoring and blocking at Bank's end.	Could you please clarify the intended use case for this activity? Typically, fake credential injection is part of fraud monitoring rather than a standard DRP/ASM capability. CloudSEK's platform already provides strong coverage against phishing through fake domain detection, fraudulent app monitoring, and coordinated takedown support, which allows the Bank to monitor and block malicious activity at its end. Your clarification will help us confirm whether this requirement should remain within DRP/ASM scope.	Clause is not refering to this RFP
58		7.3.2.7	Point 5	The feed should provide but not limited to: a) Risk lists of vulnerabilities with a configurable update frequency within 24 hours b) Risk lists of Malicious IP, Malicious Domain, URL and Hash with an update frequency in very short TAT. c) Contextual and actionable intelligence with evidence to facilitate bank's team to take necessary action d) Threat actor grouping along with TTP attribution e) The proposed solution shall provide the following types of feeds: i Malicious IP addresses having high IP Reputation ii Application layer scanning tools iii Network port scanners iv Vulnerability probers v Malware propagation sources vi Advanced URL Reputation f) Threat Intelligence feed must provide basic attributes as part of data feeds based on availability like i IP ii Domain, iii Hostility iv Reputation v Confidence vi Behavior vii Listing over a 90-day window viii Geo-location Attributes ix Industry Attributes x IP/Domain Ownership Attributes xi IP/Domain Registration Attributes xii Attack Behavior Details xiii Malware Behavior Details xiv Phishing Behavior Details xv Fraud Behavior Details xvi Bot Behaviour Details xvii CnC Behavior Details	ii. Application layer scanning tools (Partially Compliant – limited coverage, detected when linked to campaigns or exposed infrastructure but not as a standalone scanner list) iii. Network port scanners (Partially Compliant – similar limitation as above) iv. Vulnerability probers (Partially Compliant – contextual detection only)	Clause is not refering to this RFP
59		7.3.2.7	Point 7	TI feeds should be sourced from actual attacks including inspection of decrypted TLS network traffic (as opposed to synthetic environments or honeypots) happening on Threat Intelligence Feed Provider's sensor network.	We would like to seek clarification on whether the expectation is that providers must actively decrypt all TLS traffic traversing their sensor network, or if the intent is simply that the intelligence should be derived from genuine, real-world attack traffic as opposed to synthetic sources like honeypots. This distinction will help us ensure our interpretation is aligned with the actual intent and that our capabilities are mapped appropriately.	Clause is not refering to this RFP
60		15.21	Total 50,000 sustainable EPS/ 2.06 TB per day (Whichever is higher)of data ingestion from the outset scalable to Total 100,000 sustainable EPS/ 4.32 TB per day (Whichever is higher) at DC & DR	SIEM	For manpower sizing what will be the number of EPS which need to be considered, please clarify	Clause is not refering to this RFP
61			Centralized IT Infrastructure	Infrastructure management	Who will manage the old and newly deployed infrastructure, who is manging the helpdesk. Also help with list of tools deployed for ITSM, Monitoring etc.	Clause is not refering to this RFP
62		General		FMS Resources	can you please specify the number of resources required against each technology or is it completely under bidder discrition to decide the number of people	Clause is not refering to this RFP
63		General		FMS Resources	Will the billing of deployed resources be released based on the solution uptime SLA or resource availability as per the required service window? Bidder understanding is resources billing will start from date of deployment. Please clarify	Clause is not refering to this RFP
64		General		FMS Resources	what will be we are minimum qualification for the deployed resources, is there any certification required or interview from bank required. Will it be remote or onsite support model	Clause is not refering to this RFP
65		General		Integration	Please provide volumes of the solutions /tools to be integrated into the NG SOC solution	Clause is not refering to this RFP
66		General		use case management	What are the number of use cases / playbooks to be developed during a year? What are the current number of use cases deployed ? What is the current ratio of False Positives	Clause is not refering to this RFP
67		General		parser	Are there any custom parsers currently utlised for log ingestion etc. What technologies were these utilised for?	Clause is not refering to this RFP
68		8	Contract Period	The bank may, at its sole discretion, extend the contract for an additional period of two years, in one-year increments tranches. During the extension period, the annual rates of respective support components shall not exceed 15-20% of the last year's support components (ATS/ AMC/ O&M/ Subscription/ Services) prices.	It is requested that the annual rates of the support components shall be negotiated and agreed upon mutually.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
69		13.1	Assignment & Subcontracting	The selected bidder shall not subcontract or permit anyone to perform any of the work, service or other performance required under the contract.	We request that subcontracting be allowed given the scope of services.	No Change, Please be guided by the RFP
70		13.2	Delays in the Bidder's Performance	The bidder must strictly adhere to the schedule, as specified in the purchase contract/purchase order, executed between the Parties for performance of the obligations, arising out of the purchase contract and any delay in completion of the obligations by the Bidder will enable Bank to resort to any or both of the following: a. Claiming Liquidated Damages b. Termination of the purchase agreement fully or partly and claim liquidated damages. c. Execution of Bid Declaration Form / Invoking EMD or Performance Bank Guarantee	We request that a notice cum cure period of atleast 30 days be provided to the bidder to rectify any breach/delay.	No Change, Please be guided by the RFP
71		13.4	Dispute Resolution	If any dispute, difference or claim arises between the parties hereto in connection with the validity, interpretation, implementation or alleged breach of the terms of this Agreement or anything done or omitted to be done pursuant to this Agreement, the Parties shall attempt in the first instance to resolve the same through negotiation. If the dispute is not resolved through negotiation within 30 (thirty) days after commencement of discussions, then, the parties shall be at liberty to approach competent court of law at Delhi for adjudication of the disputes.	We request that the any dispute arising between the parties under the RFP/agreement be referred to arbitration, and the arbitration proceedings be conducted in accordance with the Arbitration and Conciliation Act,1996 and the Rules thereunder (as amended from time to time). Further, the arbitration be conducted by a sole arbitrator to be appointed mutually by the Parties. The seat and venue of arbitration be New Delhi, and the arbitral proceedings be conducted in English. We request changes in the clause to indicate the above.	No Change, Please be guided by the RFP
72		13.15	Order Cancellation	The Bank reserves the right to cancel the contract placed on the selected bidder and recover the expenditure incurred by the Bank on the following circumstances: a) Non submission of acceptance of order within 7 days of order. b) Excessive delay in execution of orders placed by the Bank. c) The selected bidder commits a breach of any of the terms and conditions of the bid. d) The bidder goes into liquidation voluntarily or otherwise. e) An attachment is levied or continues to be levied for a period of 7 days upon the effects of the bid. f) The progress made by the selected bidder is found to be unsatisfactory. g) If deductions on account of liquidated Damages/penalties exceeds more than 10% of the total contract price. h) If found blacklisted by any Govt. Department / PSU / other Banks / CERT-In, during contracted period. i) Non satisfactory performance of the Project in terms of affecting the Core Systems of the Bank or the Core Business of the Bank and the functioning of the Branches/Offices of the Bank.	1. Please clarify what you mean by "recovering expenditure"? 2. We request that a notice cum cure period of atleast 30 days be provided to the bidder in the event of termination for any default.	Clause is not refering to this RFP
73		13.15	Order Cancellation	Bank shall serve the notice of termination to the bidder at least 30 days prior of its intention to terminate services without assigning any reasons.	We request that a period of atleast 90 days be given before termination of the contract for convenience. Also, please confirm that PSB shall additionally pay to the Bidder for all work done till the date of termination, as well as for the orders already placed with OEMs/Licensors, which orders cannot be cancelled with the OEMs/Licensors, cancellation costs, if any, levied by the OEMs/Licensors, and logistical and administrative expenses, if any, incurred by the Bidder on account of such cancellations, which expenses shall be billed on actuals. Further, if the Bidder is providing any products/goods on opex or lease model, then PSB shall pay the Bidder the residual value of the products.	No Change, Please be guided by the RFP
74		13.15	Order Cancellation	The Bank reserves the right to recover any dues payable by the selected bidder from any outstanding amount to the credit of the selected bidder, including the pending bills and security deposit, if any, under this contract.	We request that any dues paayble only be recovered/adjusted with any liquidated damages or penalties levied against the bidder, and not against any other amount payable to the bidder for the services rendered.	No Change, Please be guided by the RFP
75		N/A	N/A	N/A	We request that the following clause on non-solicitation be added in the contract: "During the term of the contract and for a period of one (1) year following its termination, the Bank shall not directly or indirectly, either through itself or through any of its service providers or vendors, solicit or engage in any capacity, any personnel or employee or resources of the bidder, engaged in rendering any services or deployed at the Bank'a location. However, this will not apply to personnel who independently respond to general job opening postings (such as general newspaper advertisements, employment agency referrals and internet postings etc.) not directly targeting such personnel/employee.	Clause is not refering to this RFP
76		SCOPE OF WORK		At the end of the implementation, the bidder has to arrange for a Certificate from the OEM, certifying that the implementation has been done by OEM"s Resources and the deployed solution meets all the technical/functional specification of the solution as sought in the RFP.	Kindly clarify if Bidder is expected to perform the implementation or respective OEM?	Clause is not refering to this RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
77		7.11.3 NextGen SOC operations		The bidder should use bank provided Ticketing tool identified from time to time for ticketing system, tracking instructions received from application/asset owners like integration, VAPT, incident management etc. Instruction/actionable for the day-to-day operation within the NEXTGEN SOC team should be routed through such tool. Such entries in the ticketing tool should be able to provide activities/jobs completed, pending, pending at which/whose end etc. The performance & turnaround time/efficiency of onsite personnel resource would also be evaluated from the MIS generated from this tool/system	Kindly clarify if Bidder is expected to provide an ITSM tool or the bank will extend access/ integration with bank owned existing or future solution to the bidder.	ITSM Tools (OEM: manage Engine) would be provided by the bank
78		7.3.1.1 Security Information and Event Management		Log Collection - Logs from all devices / appliances / servers / applications / databases/IT sources located at the geographically dispersed location should be collected. Bidder should develop the baseline for the level of logs to be enabled from different components of IT infrastructure assets. Only in the case where remote log collection is not feasible, Bidder should install agent on the servers and applications for collection of logs. All the Raw Logs collected by Log Collection module should be stored in S-BDL	Bidder understands that PSB expects that architecture should have multi-tier, distributed, high availability (DC and DR) deployment, Kindly clarify if the High Availability should be maintained between both DC and DR as well or provision only for separate DC and DR High availability devices locally?	Clause is not refering to this RFP
79		nnexure 21: Sizing/Volumetrics		Total 50,000 sustainable EPS/ 2.06 TB per day (Whichever is higher) of data ingestion from the outset scalable to Total 100,000 sustainable EPS/ 4.32 TB per day (Whichever is higher) at DC & DR	Do we need to consider licenses starting 50,000 EPS or 100,000 EPS from day one? Or only hardware scalable up 1Lac EPS?	Please refer Addendum for revised clause
80		7.8.5 Deployment and Go-Live - Activities are to be performed by Respective Solution OEM (supported by bidder)		Red Teaming (or Purple Teaming) will be conducted by the bank or bank's appointed partner's after UAT, but prior to Go-Live or as part of security hardening and validation phase	Kindly clarify the following: 1. After deployment is Bidder expected to perform Red Teaming exercise or the bank ? 2. Should red teaming as a Service be provided by the bidder or any OEM specific license be extended to the bank?	Clause is not refering to this RFP
81					Kindly clarify should bidder consider the volumes which are shared by the bank in RFP document or additional volumes are to be considered for licensing for the deal tenure	Clause is not refering to this RFP
82		7.3.2.8 Threat hunting services			What is the frequency for Threat hunting services (quarterly/bi-annually/ Annually)	Clause is not refering to this RFP
83		7.4 Migration		The Respective OEM along with the bidder is expected to migrate the current logs of the existing solution to the proposed SIEM tool	Since every SIEM solution stores logs in their unique format, will the bank provide logs in the raw format for migration?	Clause is not refering to this RFP
84		7.7.3 Backup Infrastructure			Kindly clarify the following: 1. Is backup required at both DC and DR sites locally? 2. Please elaborate what does backup of data mean? Is the bidder expected to bring additional backup solution such as tape library, etc? 3. Is the bidder required to perform/propose one-time backup or continuous backup solution?	Clause is not refering to this RFP
85		7.8.6.1 Quality Assurance		Test Preparation	Kindly clarify the following: 1. If the bank wants to perform UAT for single solution or entire proposed solution? 2. For testing is bidder expected to consider other components as well such as routers, switches, firewalls, etc.?	Clause is not refering to this RFP
86					As part of the license procurement, does bank require any read only license for SOAR ?	Clause is not refering to this RFP
87		nnexure 21: Sizing/Volumetrics		XDR (Extended Detection and Response) solution for 12,000 users with a throughput requirement of 10 Gbps	Pls clarify the status of the 12,000 users/ endpoints – are they on-premise, cloud-based, or raming users? How do we deploy the agent to all endpoints? What existing solution, like AD, GPO, etc. is in place?	Please refer addendum for revised Volumetrics
88		nnexure 21: Sizing/Volumetrics		VA&LM Minimum Numbers of IPs: 2500	Pls clarify the web applications count.	Clause is not refering to this RFP
89		7.4 Migration		The Bidder shall be solely responsible for maintaining and managing the existing solutions and services until the successful go-live of the proposed solution. During this period, the Bidder shall ensure full compliance with the Service Level Agreements presently in force with the existing vendor.	Pls let us know the existing license status? We need a ticketing dump from the last 6-12 months for our analysis	Clause is not refering to this RFP
90		General		Passive	who will provide the rack space, power, and passive cabling for the new solution implementation?	Clause is not refering to this RFP
91		Project timelines		A) Hardware & Software Delivery & Installations	Pls confirm this timeline is for the delivery of hardware and software, and the basic installation related to infrastructure readiness.	Clause is not refering to this RFP
92					Request to modify this timeline of table (A) to T0+4 Month instead of T0+3 month	Clause is not refering to this RFP
93		Project timelines		B) Product Implementation Timelines: The timelines are applicable to each of the proposed products. (Milestone 1: SRS, HLD, LLD Signoff of Respective application) - T1= T0+2.5 Month	Request to modify this timeline of table (B) to T1=T0+3 Months	Clause is not refering to this RFP
94				Milestone 2: Implementation, Configuration, UT & SIT. - T2 = T1+2.5 Month	Request to modify this timeline of table (B) to T2=T1+6 Months	Clause is not refering to this RFP
95				C) Services Implementation (One time) Timelines: Milestone 2: Installation & configuration of software/solution/tools. - T2= T0+1.5 Month	Request to modify this timeline of table (C) to T2=T1+1.5 Month	Clause is not refering to this RFP
96		15.21		Total 50,000 sustainable EPS/ 2.06 TB per day (Whichever is higher)of data ingestion from the outset scalable to Total 100,000 sustainable EPS/ 4.32 TB per day (Whichever is higher) at DC & DR	For manpower sizing what will be the number of EPS which need to be considered, please clarify	Clause is not refering to this RFP
97		Centralized IT Infrastructure		Infrastructure management	who will manage the old and newly deployed infrastructure, who is manging the helpdesk. Also help with list of tools deployed for ITSM, Monitoring etc.	Clause is not refering to this RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
98		7	Scope of Work	The solution and instances deployed within the bank's infrastructure shall be extended to the Virtual Private Cloud (VPC) environment. This extension ensures that the monitoring, security, and management capabilities are consistent across both on-premises and cloud-based resources. Example SIEM Log collector instance would be deployed on VPC as well to collect the VPC logs.	We recommend bank to have VPC created on-premises and integration with cloud based solution to be limited to SAAS services only.	Clause is not refering to this RFP
99		7.2	SOC solutions & Services	# Solution & Services Deployment Mode 1 SIEM On-premise/ On-Cloud 2 SOC Big Data Lake On-premise/ On-Cloud 3 SOAR On-premise/ On-Cloud 4 UEBA On-premise/ On-Cloud 5 Decoy/Honeypot On-premise/ On-Cloud 6 XDR On-Cloud 7 Threat Intelligence Platform On-premise/ On-Cloud 8 Vulnerability Assessment, lifecycle & management On-premise 9 Application Security Testing Tool On-premise 10 Cloud Security (CSPM) Tool On-premise/ On-Cloud	We recommed to remove deployment mode as On-cloud for listed solution & services having on-premises / on-cloud option	Clause is not refering to this RFP
100		7.3.1.1	Architecture/Deployment model: Point 9	All Log exports (structured/unstructured) from Cloud SIEM should be pushed into Big Data Lake and on-premise storage solution periodically and on a Real time basis.	Any egress data from cloud based VPC to on-premises will incur high data transfer cost. Backup will also be covered for the solution and restore back to on-premises will incur high data transfer costs. We recommend SIEM solution to be deploymend on-premises	Clause is not refering to this RFP
101		7.3.1.2	SOC Big Data Lake (S-BDL), Architecture/Deployment model: Point 6	The analytics solution for S-BDL can be deployed either on-premises or on-cloud, depending on the bidder's proposed architecture. However, if a cloud-based analytics solution is proposed, the bidder must provide detailed architecture that clearly demonstrates how all logs, data, and other relevant information will also be stored on-premises in a readable format, and is regularly tested to ensure data sanctity and integrity.	Recommend to removed option for cloud-based solution which will incur high costs for data transfer (backup restore, log collection from cloud to on-premises, cloud infra and storage cost)	Clause is not refering to this RFP
102		7.3.1.3	SOAR (Security Orchestration, Automation, & Response), Architecture/Deployment model: Point 3	In case of bidder proposing the SOAR (Cloud Based)	Recommend to removed option for cloud-based solution which will incur high costs for data transfer (backup restore, log collection from cloud to on-premises, cloud infra and storage cost)	Clause is not refering to this RFP
103		7.3.1.4	UEBA (User and Entity Behavior Analytics), Architecture/Deployment model: Point 3	In case of bidder proposing the UEBA (Cloud Based)	Recommend to removed option for cloud-based solution which will incur high costs for data transfer (backup restore, log collection from cloud to on-premises, cloud infra and storage cost)	Clause is not refering to this RFP
104		7.3.1.5	Extended, Detection and Response (XDR): Architecture/Deployment model: Point 3	In case of bidder proposing the XDR (Cloud Based)	Recommend to removed option for cloud-based solution which will incur high costs for data transfer (backup restore, log collection from cloud to on-premises, cloud infra and storage cost)	Clause is not refering to this RFP
105		7.3.1.6	Decoy/HoneyPOT, Architecture/Deployment model: Point 3		Recommend to removed option for cloud-based solution which will incur high costs for data transfer (backup restore, log collection from cloud to on-premises, cloud infra and storage cost)	Clause is not refering to this RFP
106		7.3.1.7	Threat Intelligence Platform, Architecture/Deployment model: Point 2	Bidder to ensure adequate storage is factored on cloud/On-premise to store the data, logs (structured & unstructured) on primary cloud/On-Premise (SSD/NvME) storage for period defined in the Volumetrics sheet (Annexure 21).	Recommend to removed option for cloud-based solution which will incur high costs for data transfer (backup restore, log collection from cloud to on-premises, cloud infra and storage cost)	Clause is not refering to this RFP
107		7.3.1.8	Vulnerability assessment, Lifecycle & management Tool: Architecture/Deployment model: Point 3	Bidder to ensure adequate storage is factored on cloud/On-premise to store the data, logs (structured & unstructured) on primary cloud/On-Premise (SSD/NvME) storage for period defined in the Volumetrics sheet (Annexure 21).	Recommend to removed option for cloud-based solution which will incur high costs for data transfer (backup restore, log collection from cloud to on-premises, cloud infra and storage cost)	Clause is not refering to this RFP
108		7.3.1.10	Cloud Security (CSPM) Tool: Architecture/Deployment model: Point 1, 2 & 3	1) The proposed solution must be deployed with instances/agent/agentless deployed on Cloud VPCs for monitoring, compliance, and policy enforcement 2) Bidder to ensure adequate storage is factored on cloud/ On-premises to store the data, logs (structured & unstructured) on primary cloud/ On-Premises (SSD/NvME) storage for period defined in the Volumetrics sheet (Annexure 21). 3) In case of bidder proposing the CSPMs (Cloud Based)	Most of the CSPM solutions are designed for hyperscalers and since bank has very low foot print on cloud, the deployment should be primarily on-premises and extended to cloud.	Clause is not refering to this RFP
109		7.4	Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	Migration of all existing solutions (Existing SOC and security solutions to proposed NextGEN SOC and other security solutions)	What is the current platform running existing SOC setup	Clause is not refering to this RFP
110		7.4	Migration - Activities are to be performed by Respective solution OEM (supported by bidder)	Respective OEM along with the bidder is required to inter-work, liaison with existing vendor for having a smooth migration from existing Solution to the bidder proposed application/infrastructure.	Recommend to incude live migration of infrasturue without any downtime from existing to new setup to prevent any data loss from manual efforts.	Clause is not refering to this RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
111		7.5	Non-functional requirements, point 4	Scalability - All components of the solution must support scalability to provide continuous growth to meet the requirements and demands of BANK. The Solution should scale in a linear fashion and behave consistently with growth in data, number of concurrent users etc.	The solution must use memory optimisation features such as Transparent Page Sharing, Memory Balooning & Memory tiering for deploying more workloads on a physical server	Clause is not refering to this RFP
112		7.5	Non-functional requirements, point 5	Availability - All components of the solution must provide adequate redundancy to ensure high availability. The solution shall have built in redundancy in terms of both the hardware and connectivity so that service is not impacted and is available 24x7.	The solution must have no single point of failure architecture. Example if any virtulization solution is used, it should not have downtime during any Virtulization OS patch and hardware maintenance activity.	Clause is not refering to this RFP
113		7.5	Non-functional requirements, point 7	Security: Proposed solution should provide role-based security, encryption of data-at-rest, data in use, data-in-transit, and data on backup media.	The solution must provide a purpose-built hypervisor that installs directly on the bare metal x86 server hardware with no dependence on a general-purpose OS for reliability and security.	Clause is not refering to this RFP
114		7.7	IT Infrastructure requirements, point 2	2. If the proposed solution is cloud-based, the bidder must accurately right-size the cloud infrastructure to meet all performance, capacity, and SLA requirements outlined in the RFP. The design should ensure availability within the primary cloud site, incorporating failovers, backups, and health monitoring, while also including a disaster recovery plan with a secondary site that meets the defined requirement as stated in the RFP. The proposal should include detailed architecture diagrams and a sizing justification.	The sizing justification by the bidder to go with cloud based solution should be backed by submitting a 5 year TCO as per the RFP timeline. The TCO must include cloud infrasturture cost (storage & compute), DR setup, data transfer, backup recovery, log transfer to on-prem and security services (deployed from security perspective (CSPM,etc))	No Change, Please be guided by the RFP. Bidder based on their design is required to propose the solution complying with the terms of the RFP
115		7.7	IT Infrastructure requirements, point 23	The bidder is responsible to provide the correct sizing of compute, network, and storage, IOPS including server etc. in collaboration with the proposed OEM whose solution/technologies are proposed for Nextgen SOC for successful deployment. Bidder and OEM should also account for scalability and future growth of the Bank to arrive at sizing for the Contract period.	The bidder to consider any infra memory optimisation features such as Transparent Page Sharing, memory tiering, memory balooning while proposing.	No Change, Please be guided by the RFP
116		7.7.1	Compute Infrastructure, point 7	The virtualization architecture must ensure no single point of failure. In case of one instance / node is deployed on server 1 then the second instance / node of the same environment of the solution should not be deployed in the same physical server.	The proposed solution must be able to automatically meet VM resource demands by distibuting load across virtlization cluster.	No Change, Please be guided by the RFP
117		7.7.1	Compute Infrastructure, point 2	The hardware sized should be redundant, both horizontally and vertically scalable, fault tolerant and designed for high availability.	The proosed solution must cover storage failure scenario (APD & PDL) and network failure sceanrios as well for ensuring high availability	No Change, Please be guided by the RFP
118		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management	1.7	The Solution should have an option of defining the online data retention period so to retain results for a defined and configurable period of time after which the results are expired and archived into another querriable database automatically.	After a configured time the data is deleted to free up storage space for latest data, if this is to be retained even the configurable time such as 180 days, tool should have reports, APIs available for data to be exported to customer storage systems. Hence, request to update as following ------ "The Solution should have an option of defining the data retention period so to retain results for a defined and configurable period of time. If data retention is required post the configurable time, API based data extraction and storage at the customer location should be supported."	Clause is not refering to this RFP
119		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management	3.1	The Solution should provide mechanism to integrate with SIEM, SOAR, Threat Management systems, NACs etc..	Please share details (Vendor/Tool/Version) of the SIEM, SOAR, TM and NAC solution you would want to integrate with.	Clause is not refering to this RFP
120		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management	3.2	The solution should be able to integrate with PAM solutions to perform secure credential-based VA.	Please share details (Vendor/Tool/Version) of the PAM solution you would want to integrate with	Clause is not refering to this RFP
121		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management	3.3	The solution should be able to integrate with IT ticketing and workflow systems to streamline and accelerate the handover of information and to obtain visibility into the remediation process.	Please share details (Vendor/Tool/Version) of the IT ticketing solution you would want to integrate with.	Clause is not refering to this RFP
122		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management - Identity Threat Detection & Response	7.2	Identity Threat Detection Solution should Identify currently vulnerable identities and associated credentials that would provide an attack path to an attacker post initial compromise.	To ensure the solution is capable of performing pre-breach and proactive identity security which is preferred over post-breach/reactive security, we request the clause to be as following - “ Identity Threat Detection Solution should identify currently vulnerable identities and associated credentials that would provide an attack path to an attacker prior to initial compromise.”	Clause is not refering to this RFP
123		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management - Identity Threat Detection & Response	7.6	Identity Threat Detection Solution should must automatically prioritize and remediate the riskiest identities to preemptively cut off what attackers need (and expect to find) to move undetected within the network.	We understand your are asking technology to provide remidiation guidance and scripts rather than remidation - Identity Threat Detection Solution must automatically prioritize the riskiest identities and provide tailored remediation guidance and customized scripts to preemptively cut off what attackers need (and expect to find) to move undetected within the network.	Clause is not refering to this RFP
124		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management - Identity Threat Detection & Response	7.7	Identity Threat Detection Solution Should detect and respond to active threats with high fidelity (low false positives and false negatives).	Since most of the identy related challenges are not suggested to be autoremidiated, we request the clause to be as following - Identity Threat Detection Solution Should detect and provide tailored remediation guidance along with customized script option preemptively to cut off active threats with high fidelity (low false positives and false negatives).	Clause is not refering to this RFP
125		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management - Identity Threat Detection & Response	7.8	Identity Threat Detection Solution should collect source-based forensic data in real-time from compromised machines to assist with incident response.	This is an EDR/XDR specific requirement to be able to collect data from source machines and should be part of EDR/XDR solution only. We request to remove this clause from here	Clause is not refering to this RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
126		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management - Identity Threat Detection & Response	7.9	Identity Threat Detection Solution should provide contextual information—who, what, when and how—to inform all stages of the attack chain.	This is an EDR/XDR specific requirement to be able to collect data from source machines and should be part of EDR/XDR solution only. We request to remove this clause from here	Clause is not refering to this RFP
127		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management - Identity Threat Detection & Response	7.10	Identity Threat Detection Solution should provide deep insights into both the potential and used privilege escalation and lateral movement steps in an attack.	Used privilege escalation investigation is a feature of post breach investigation and should be done at EDR/XDR end, we request the clause to be as following - Identity Threat Detection Solution should provide deep insights into both the potential escalation and lateral movement steps in an attack.	Clause is not refering to this RFP
128		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management - Active Directory Vulnerability Discovery and Remediation	8.1	Identity Threat Detection Solution should discover and provide remediation for, insufficient or improper PAM configuration and management of service-account, local-administrator, and privileged-domain credentials	We request this to be as following for us to participate- Identity Threat Detection Solution should discover and provide remediation for management of service-account, local-administrator, and privileged-domain credentials along with identification of whether PAM rotated the password correctly or not by identifying too many similar passwords.	Clause is not refering to this RFP
129		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management - Active Directory Vulnerability Discovery and Remediation	8.2	Identity Threat Detection Solution should discover and provide remediation for, unintentional creation of shadow admin accounts that have excessive privileges.	We suggest to update as following for you to have a more comprehensive coverage on the ask ---- Identity Threat Detection Solution should discover and provide remediation for unintentional creation of shadow admin accounts that have excessive privileges, specifically including users granted administrative access through direct ACEs in Active Directory, GPO delegation, or user rights assignments in GPOs.	Clause is not refering to this RFP
130		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management - Active Directory Vulnerability Discovery and Remediation	8.3	Identity Threat Detection Solution should discover and provide remediation for, Improper termination of RDP sessions	This is not an identity security specific requirement. We request to remove this clause.	Clause is not refering to this RFP
131		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management - Active Directory Vulnerability Discovery and Remediation	8.4	Identity Threat Detection Solution should discover and provide remediation for, stored credentials on endpoints—including web browsers, SSH, FTP, PuTTY, command lines, and databases—that cache credentials.	This is an EDR/XDR specific requirement and should be part of EDR/XDR solution only. We request to remove this clause and this to EDR/XDR portion	Clause is not refering to this RFP
132		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management - Active Directory Vulnerability Discovery and Remediation	8.5	Identity Threat Detection Solution should Identify, Misconfigured accounts, Legacy app accounts, Stale accounts, password policy violations, Kerberoastable credentials, unmanaged user accounts, unmanaged service accounts	Request the clause to be as following for a more comprehensive solution ------ Identity Threat Detection Solution should identify misconfigured accounts, stale accounts, hidden privileged accounts, password policy violations, Kerberoastable credentials, user accounts, service accounts, machine accounts, and Entra ID applications.	Clause is not refering to this RFP
133		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management - Active Directory Vulnerability Discovery and Remediation	8.6	Identity Threat Detection Solution should Provide continuous monitoring and customizable, automated business rules to eliminate security policy violations, such as: • Stale or disconnected RDP sessions • Stored credentials to sensitive assets • Local-admin accounts • Cached credentials stored in browsers, Windows and other systems.	Request the clause to be as following for a more comprehensive and identity security specific solution ------ Should support custom single monitoring query to monitor changes such as below in an inclusive AND query * irregular service accounts configuration * Service account with privileges * weak password * have unconstrained delegation configured)	Clause is not refering to this RFP
134		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management - Active Directory Vulnerability Discovery and Remediation	8.7	Identity Threat Detection Solution should be available through rack-mountable physical appliances/servers.	Physical appliances come with a plethora of issues w.r.t cost, RMA, scalability etc. We request this clause to be following for you to have a more manageable, cost-efficient and scalable solution ------ Identity Threat Detection Solution should be available through virtual machines.	Clause is not refering to this RFP
135		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management - Active Directory Vulnerability Discovery and Remediation	8.10	Identity Threat Detection Solution should detect all types of attack vectors including but not limited to pre attack reconnaissance,zero- day attacks, privilege escalation prevention, lateral movement, data theft	Request the clause to be as following for a more comprehensive solution ------ Identity Threat Detection Solution should detect all types of attack vectors including but not limited to pre-attack reconnaissance, zero-day attacks, privilege escalation prevention, lateral movement, and data theft. The solution should provide temporal correlation of detected attacks and maintain comprehensive change tracking for Active Directory modifications during specific timeframes, including historical attribute values and sysvol file changes.	Clause is not refering to this RFP
136		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management - Active Directory Vulnerability Discovery and Remediation	8.11	Identity Threat Detection Solution should detect multiple attacks simultaneously.	Request the clause to be as following for a more comprehensive solution ------ Identity Threat Detection Solution should detect multiple attacks simultaneously by monitoring suspicious changes across Active Directory GPOs, SYSVOL files, AD schema modifications, certificate alterations, and object attribute changes.	Clause is not refering to this RFP
137		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management - Active Directory Vulnerability Discovery and Remediation	8.12	Identity Threat Detection Solution should discover vulnerable identities, exposures and misconfigurations	Request the clause to be as following for a more comprehensive solution ------ Identity Threat Detection Solution should discover vulnerable identities, exposures and misconfigurations in both Entra ID and on-premises Active Directory, with prioritization based on the most important assets determined by the number of access rights and entitlements available to each user.	Clause is not refering to this RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
138		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management - Active Directory Vulnerability Discovery and Remediation	8.13	Identity Threat Detection Solution should provide insight into how a combination of these vulnerabilities can provide attack paths to crown jewel IT assets or other critical or sensitive systems	Request the clause to be as following for a more comprehensive solution ------ Identity Threat Detection Solution should provide insight into how a combination of these vulnerabilities can provide attack paths to crown jewel IT assets or other critical or sensitive systems, with automatic crown jewel identification and user-configurable definitions.	Clause is not refering to this RFP
139		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management - Active Directory Vulnerability Discovery and Remediation	8.16	Identity Threat Detection controls should begin with understanding what IT systems are a priority to protect.	Request the clause to be as following for a more comprehensive solution ------ Identity Threat Detection controls should begin with understanding what IT systems are a priority to protect by providing automated priority scoring based on multiple parameters, including on-premises Active Directory group memberships, Entra ID roles, Entra entitlements, and on-premises ACEs.	Clause is not refering to this RFP
140		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management - Active Directory Vulnerability Discovery and Remediation	8.19	Identity Threat Detection Solution should be able to pull and analyze identity data from AD, Entra ID, identity stores, PAM systems.	We request to please remove the PAM systems. We request the clause to be following for us to participate - Identity Threat Detection Solution should be able to pull and analyze identity data from AD, Entra ID, identity stores.	Clause is not refering to this RFP
141		FuncTechxxxx - Cloud Security	1	The solution must support major cloud provider like AWS, Meghdoot, Azure, Google Cloud). For all supported cloud providers, the supported solution must support ○ Agentless Scanning ○ Full audit trails of the solution ○ Granular RBAC based on account/subscription/project or custom grouping	We request to remove 'Meghdoot' from the list of supported clouds service providers for us to participate. The update clause can be as following ------ The solution must support major cloud provider like AWS, Azure, Google Cloud. For all supported cloud providers, the supported solution must support ○ Agentless Scanning ○ Full audit trails of the solution ○ Granular RBAC based on account/subscription/project or custom grouping	Clause is not referring to this RFP
142		FuncTechxxxx - Cloud Security	22	The solution must have the ability to resolve cloud misconfiguration findings via cloud-native APIs	We request for this to be updated as following - The solution must have the ability to resolve IAM related cloud misconfiguration findings via cloud-native APIs along with ability to suggest solutions for remaining cloud misconfigurations.	No Change, Please be guided by the RFP
143		FuncTechxxxx - Cloud Security	23	The solution must support integration and automation with collaboration tools, SIEM tools, ITSM tools (Manage Engine) and customizable workflows through webhook triggers.	Please share details of the SIEM tools, collaboration tools as well. The update clause can be as following if the tool list matches at your end ----- The solution must support integration and automation with collaboration tools (Teams, Slack), SIEM tools (Splunk, Qradar, Datadog) ITSM tools (Manage Engine) and customizable workflows through webhook triggers.	Clause is not refering to this RFP
144		PSBNextGENxxxxxxx - 15.21 Annexure 21: Sizing/Volumetrics	8 (VA&LM)	Minimum Numbers of IPs: 2500	As per RFP, Below are the count Servers deployed with OS, DB, Web/app component, middleware's, agents and other applications / software, private & public cloud setups, emerging technologies etc. - 2500 Database - 300 Desktops with various agents like AV, DLP, NAC, ITAM etc. - 12000 Routers & Switches - 7200 As per best practices and regulatory guidelines, it is advised to scan all the IP assets in IT Infrastructure. Accordingly, shall we consider 22000 as assets to be scanned. Kindly guide.	Clause is not refering to this RFP
145		PSBNextGENxxxxxxx - 15.21 Annexure 21: Sizing/Volumetrics	8 (VA&LM)	Minimum Numbers of IPs: 2500	Given the ITDR solution is also part of VA & LM, please share the active user count on the AD & Entra ID for us to propose sizing of the solution.	Clause is not refering to this RFP
146		PSBNextGENxxxxxxx - 15.21 Annexure 21: Sizing/Volumetrics	8 (VA&LM)	HA (Active/Active – N+N redundant Deployment) at DC and HA (Active/Active – N+N redundant Deployment) at DR All the inline components of the solution must operate in high availability mode. In the event of any component failure, the system should automatically initiate failovers within seconds, ensuring uninterrupted functionality without requiring manual intervention. Each node/environment must be individually provisioned for full peak load Logs should be stored for 6 months on primary storage(SSD/NVME).	VA & LM is not an inline solution such as a firewall or IPS hence, it does not require to be in Active/Active or Active/Hot Standby. Additionally Active/Active solution won't even be possible due to dual database maintenance requirements and bidirectional sync at any point between sites. We suggest the update to the clause as following for us to participate ---------HA (Redundant Scanner Deployment (N+N)) at DC and Cold Standby HA (Redundant Scanner Deployment (N+N)) at DR It should be possible to utilize the redundant scanners at DC as well as DR in case the primary scanners go down. In the event of any component failure, it should be possible for DR console to be brough up with manual intervention. It should be possible to scan and analyze DC as well as DR components from DC central console and vice versa in an event of failover where DR console is active as primary. Each node/environment must be individually provisioned for full peak load. Logs should be stored for 6 months on primary storage(SSD/NVME).	Clause is not refering to the aforementioned RFP
147		PSBNextGENxxxxxxx - 15.21 Annexure 21: Sizing/Volumetrics	10(CSPM)	At least 20 VMs (VPCs)	Need to have the total as well as maximum cloud workloads count for license consideration and solution sizing proposal.	No Change, Please be guided by the RFP
148		PSBNextGENxxxxxxx - 15.21 Annexure 21: Sizing/Volumetrics	7.3.1.10 Cloud Security (CSPM) Tool	The tool logs storage should be deployed on bank's DC & bank's DR. In this setup, only communication should be established between the on-premises CSPM console and the bank's cloud VPCs via CSPM Agent or Interface on VPCs.	Please confirm if these lines are not to be applied to SaaS based Cloud CSPM providers given the console there will be on cloud along with storage and there the HA is based on the availability SLA. The communication should also be between SaaS CSPM and banks Cloud VPCs via the APIs.	Clause is not refering to this RFP
149		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management	7.1	Identity Threat Detection solution can be proposed as either a single solution or combiniation of multipleof solution	Lifecycle Management should be from same OEM as Vulnerability Management	Clause is not refering to this RFP
150		FuncTechxxxx - Vulnerability Assessment & Lifecycle Management			We understand bank is asking for a solution that is OnPrem, Agentless and will work without dependency of any other agent on endpoint. Please confirm understanding	Clause is not refering to this RFP
151		Operation & Maintenance Phase	7.10 Resource Requirement	"The proposed resource should have experience of managing at least 1 NextGEN Security solution in at least 2 PSU/ PSE/ Govt. Department/ BFSI organizations/ Regulatory Bodies of India."	"The proposed resource should have experience of managing at least 1 SOC solution in at least 2 PSU/ PSE/ Govt. Department/ BFSI organizations/ Regulatory Bodies of India."	Clause is not refering to this RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
152		Anti-phishing, Anti-rogue app, anti-malware etc. Brand protection and Monitoring Dark Web Monitoring	Panalities	a. Detection of phishing sites, rogue app, brand abuse, malicious content etc. elaborated in RFP > 85% b. Site take-down time for identified Phishing URLs – Resolution within 8 hours c. Site take-down time for Brand Abuse – Resolution within 36 hours d. Enrichment: Cybercrime – Resolution within 1 Hours e. Enrichment: Nation State– Resolution within 1 Hours f. Any other (Like Interaction, Ransomware, Malware Reverse Engineering etc.) – Resolution within 1 Hours (From the time of reporting the request / issue through phone call / email / web-based portal)	For takedowns, every vendor is dependent on the third-party platform where the post is hosted. Therefore, we cannot commit to this timeline as it is not reasonable	Please be guided by the RFP
153	1	Primary Storage	5	Proposed storage solution should be offerred with minimum 2 controllers with minimum 256 GB DRAM Cache memory on the entire storage Solution. The solution should scale to atleast 512GB Cache memory by adding additional controller.	Change To: Proposed storage solution should be offerred with minimum 2 controllers with minimum 128 GB DRAM Cache memory on the entire storage Solution. The solution should scale to atleast 256GB Cache memory by adding additional controller. Explaination: Cache ask should be Reduced as cache of 64GB or less per controller (128GB total) is enough as the latest CPUs, high-speed memory, and Gen 5 PCIe cards deliver the required performance efficiently. Modern storage controllers optimize cache usage, and industry benchmarks confirm that asked performance can be achieved with lower memory. This reduction not only meets technical needs but also decreases hardware, power, and cooling costs, resulting in a lower TCO for the solution	No Change, Please be guided by the RFP
154	1	Backup Solution	16	The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data over a secure, API-based disk-to- disk (D2D) connection.	Change To: The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data using standard Data protocolos such as FC, ISCI, NFS, S3 Expalination: This specific ask qulifies only specific backup appliance not any target storage as enterprise storage do not support data ingestion using API rather laverage protocols such as FC, ISCI, NFS, S3.	Please refer addendum for revised clause
155	1	Backup Solution	25	The Proposed Appliance/Backup Storage must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism	Change To:The Proposed Appliance/Backup Solution must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism Explaination: Proposed ask should be from Solution instead of storage as any storage does not offer file-level checksum reporting for backup files. This is typically a function of the backup software (e.g., Commvault, Veeam) that stores backups on storage.	Please refer addendum for revised clause
156	1	Primary Storage	21	If the OEM proposes effective storage capacity, then DRR should be applicable for the entire contract period. Incase, the DRR is not achieved anytime during the contract period, the OEM is liable to supply the additional drives/capacity to meet the required performance and effective capacity at no additional cost to the bank.	Query:Bank should provide workload details such as if data would encrypted or non-encrypeted, compressed or non-compressed and type of DB, VM etc. Explaniation: It would help OEM to size solution with correct DRR commitment.	Bidder/OEM shall assess the workload details and other relevant technical requirements and propose a suitably sized and architected solution meeting all requirements & terms of the RFP. The Bidder/OEM shall be responsible for sizing, performance, interoperability and adequacy of the proposed solution
157	1	Long Term Storage		Addititional Point Request	Point to be written as: Long Term Storage should support WORM (Wrte Once, Read Many) capability to have Data Immutability. Explaination: We recommend implementing WORM (Write Once, Read Many) capability for long-term backup storage to ensure data is protected against accidental deletion and ransomware attacks. Additionally, WORM functionality is required to comply with regulatory guidelines for banking institutions. Since backup storage is expected to provide WORM capability, long-term backup storage should also comply with this requirement to maintain robust data protection.	As per tender pg no. 39, point a, "*No Bank data shall be deleted or made inaccessible before expiry of the applicable retention period (refer annexure 21) and without explicit written authorization from the Bank*" It is bidders responsibility to ensure that they comply with the tender requirement
158	1	Primary Storage Backup Storage Long Term Storage		New Point request	Point to be written as: The proposed storage systems (for all 3 storage requirements), should have launch dates within past 3 years Explainations: We recommend qualifying storage systems with a launch date within the past three years. This approach ensures a better return on investment and reliable long-term support for a period of 7 to 10 years, as required by the bank. Some OEMs are currently offering systems that are over six years old and lack a clear roadmap or support commitment, which poses a risk to long-term operational stability and longitivity.	Please refer addendum for revised clause.
159	50-52	Functional Requirements – Solutions	7.3.11 / 7.3.12 / 7.3.13	CSPM, CNAPP and CWPP requirements for cloud environments	Which cloud provider(s) are you predominantly using?	Details shall be shared with the successul bidder, the proposed solution should comply with the requirement mentioned in the RFP
160	29-34	Solution & Services Deployment Model	7.2 / 7.2.4	Solution deployment model and deployment architecture	Please clarify whether the Bank will provide the required cloud-native audit/security logs and API access/permissions for the respective cloud environments to enable assessment of the applicable security controls.	Bank will provide relevant access to bank's environment inlcuding cloud deployement currently in place
161	51-53	Functional Requirements – Solutions	7.3.12 / 7.3.13	CNAPP and CWPP requirements covering Kubernetes environments	Are you running Kubernetes workloads? If yes, are they managed or self-managed?	Details shall be shared with the successul bidder, the proposed solution should comply with the requirement mentioned in the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
162	52-53	Functional Requirements – Solutions	7.3.12 / 7.3.13	CNAPP/CWPP requirements for Kubernetes and runtime protection	Do you need Kubernetes Runtime security & enforcement as part of the CNAPP platform?	Details shall be shared with the successul bidder, the proposed solution should comply with the requirement mentioned in the RFP
163	51-52	Functional Requirements – Solutions	7.3.12.1, Point 4	API security findings shall be correlated with applications, cloud resources, workloads, identities and network resources	Do you need API security as well ? Which API Gateway are you using - cloud native service or self-hosted?	Bank currently is in process of implementing API Security, details of which shall be shared with the successul bidder, the proposed solution should comply with the requirement mentioned in the RFP
164	50	Functional Requirements – Solutions	7.3.11.1	CSPM shall provide centralized visibility across cloud assets and resources	Approximately how many cloud accounts/projects are in scope? & total VM/nodes, kubernetes clusters, no. of databases, no. of storage buckets, no. of repositories, no. of images across all repositories.	Details shall be discussed with the successful bidder
165	51-52	Functional Requirements – Solutions	7.3.12	CNAPP shall provide identity and entitlement risk assessment across cloud-native environments	If you are using Kubernetes, is IAM/WIF-based authentication enabled?	Details shall be shared with the successul bidder, the proposed solution should comply with the requirement mentioned in the RFP
166	50-53	Functional Requirements – Solutions	7.3.11 / 7.3.12 / 7.3.13	CSPM/CNAPP/CWPP cover multi-cloud, hybrid-cloud and on-premises environments	The RFP specifies CSPM/CNAPP for public cloud environments. Does the scope also include private or on-premises cloud/data-center environments, such as OpenStack or VMware?	The Solution is required for Public Cloud Ennvironment deployment
167	29-34	Solution & Services Deployment Model	7.2 / 7.2.4	Deployment model and deployment architecture for proposed solutions	Do you need a dedicated/isolated tenant/hosting of the application/platform in cloud or public SAAS (Shared infra, network database)?	Please refer addendum for the revised deployment architecture Logical tenancy is acceptable, provided that the proposed bidder/OEM ensure clear separation and isolation of the Bank's data, security telemetry, logs, alerts, configurations,
168	50-52	Functional Requirements – Solutions	7.3.11 / 7.3.12	CSPM/CNAPP cloud security, risk assessment, prioritization and remediation	Do you require cloud FinOps capability as part of CSPM/CNAPP platform to get clost improvement insights within a single unified dashboard?	No Change, Please be guided by the RFP
169	56	Functional Requirements – Services	7.4.4 – Phishing Simulation	Employee awareness, behavioural analysis, user/department risk assessment and identification of high-risk users	Are you looking for a holistic human risk management solution to continuously evaluate and monitor blended risk i.e. risk across all employees based on their actions (for e.g. capture risk when an employee is blocked by web gateway trying to access an un-authorized website etc.) along with risk of an employee based on his/her actions during phishing, vishing & smishing simulations?	The requirement is limited to employee awareness, behavioural analysis and risk assessment based on the employee's response to the phishing-simulation activities conducted under the RFP
170	Appendix 1C	Functional Compliance Sheet – Services	Smishing/Vishing requirements	Conducting simulated SMS and voice-based phishing exercises.	Please clarify the expected volume/no. of targets and frequency of both SMS and Vishing campaigns.	The Bank shall provide the campaign schedule and target population from time to time. The Bidder shall support the volumes/frequency specified in the RFP and as required by the Bank during the contract period. The solution shall be sized to support the stipulated user base and campaign requirements.
171	Appendix 1C	Functional Compliance Sheet – Services	Phishing Simulation – Data Storage	Bank data generated during phishing activities shall not be stored at Vendor location and storage shall be restricted to Bank network.	The RFP describes phishing simulation as an offsite, tool-based service. Is bank expecting dedicated/ isolated cloud SAAS deployment which means entire cloud based SAAS application including machines, middleware, database, storage be dedicated to bank?	Please refere addendum for revised clause
172	Appendix 1A	Functional Compliance Sheet (Solutions)	CSPM - S.No. 28	CTEM -- Continuous Threat Exposure Management (CTEM)	As part of CTEM - Are you looking for Attack Path Analysis after every DRIFT/CRUD - create, read, update & delete? In other words, do you expect the system to visually simulate how an attacker could pivot from a minor vulnerability to a critical cloud asset?"	No Change, Please be guided by the RFP
173	29, 35 & 259	Sections 7.2.1, 7.2.4.1(b) & 16.21.2		Deception deployment and high-availability topology Section 7.2.1 (Deception Technology): "Any agent/Enforcer/Deceptor Standalone at DC and HA, N+N, Standalone at DR." Section 7.2.4.1(b): "The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active configuration." Section 16.21.2 (Decoy): "All the inline components of the solution must operate in high availability mode. In the event of any component failure, the system should automatically initiate failovers within seconds, ensuring uninterrupted functionality without requiring manual intervention."	The RFP describes the Bank-side deception components as standalone in Section 7.2.1, point no.- 4, but it is also mentioned HA and N+N. We request the bank to kindly clarify that in case we're deploying the solution on-prem, whether Bank needs the solution in Standalone mode/HA mode/N+N mode. Section 16.21.2 (Decoy), point no.-8, Bank has asked that all the inline components of solution should be in HA mode with automatic failover capability. However, the deception solution is not inline. Hence, we request Bank to clarify if they need the Deception Solution in HA. We request the Bank to add on-prem solution also in addition to Cloud/SAAS+Hybrid.	Please refer addendum for revised clause
174	45, 261 & 262	Sections 7.3.6.2(2) & 16.21.3 - Deployment and Data Retention		Backup, restoration and log-retention requirements Section 7.3.6.2(2): "Restore the logs/data from backup for forensic investigation and as per bank requirement without any additional cost." Section 16.21.3: "Duration of the Contract (Monthly Full backup) - Long-Term Storage (LTS) - Entire Duration of the Contract." The RFP further states that applicable Monthly Full Backups shall be migrated to LTS at the Bank's DC & DR and retained for the entire duration of the contract.	We request bank to kindly confirm that if the bank will provide the storage for backup.	No Change, Please be guided by the RFP. Bidder to right size and provide all the required infrastrcuture as per RFP
175	68	Section 7.7 - On-cloud proposed solution OEM Responsibilities, Point 10		Cloud OEM certification requirement "The OEM shall have valid ISO/IEC 27001 certification and SOC 2 Type II report."	We request the bank to accept ISO/IEC 27001 or SOC 2 Type II or both.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
176	29, 32 & 35	Sections 7.2.1, 7.2.3 and 7.2.4.1(b)		Responsibility for providing the Cloud/SaaS environment Section 7.2.1 (Deception Technology): "Cloud (SaaS) + Hybrid" Section 7.2.3: "The solution shall be hosted through a Cloud Service Provider (CSP), either fully as a SaaS service or through a combination of CSP-hosted and Bank-hosted components." Section 7.2.4.1(b): "Deception Technology: The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active configuration. The Cloud/SaaS deployment shall be aligned with the applicable SLA, RTO and RPO requirements."	7.2.4.1(b) We request the bank to kindly add the on-prem implementation option also for the core component of the Deception Solution.	Please refer addendum for revised clause
177	35 & 91	Sections 7.2.4.1(b) and 7.18.1 - Compute Infrastructure, Point 1		Hardware and VM infrastructure for Bank-hosted deception components Section 7.2.4.1(b): "Deception Technology: The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active configuration. The Cloud/SaaS deployment shall be aligned with the applicable SLA, RTO and RPO requirements." Section 7.18.1(1): "Bidders must design, size, supply, implement, maintain and manage suitable compute infrastructure for all the in-scope applications/solutions proposed in the RFP response."	We request the bank to kindly add the on-prem implementation option also for the core component of the Deception Solution.	Please refer addendum for revised clause
178	31 & 35	Sections 7.2.1 Note and 7.2.4.1(b)		Required Bank-hosted deception components Section 7.2.4.1(b): "Deception Technology: The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active configuration. The Cloud/SaaS deployment shall be aligned with the applicable SLA, RTO and RPO requirements."	We request the bank to kindly add the on-prem implementation option also for the core component of the Deception Solution.	Please refer addendum for revised clause
179	66	Point No. 5 Backup Solution of Appendix 1B	Backup Solution	Proposed backup software must support Multi-Tenancy feature.	Request specification change: Proposed backup solution should support Multi-Tenancy feature Justification: As this scope of the RFP is to protect all the SoC environment, which is a single-enterprise environment rather than a shared-customer platform, enabling multi-tenancy would introduce additional network, administration, and recovery complexity without providing a meaningful security or operational benefit. We can preserve the option to introduce multi-tenancy later if independent tenants, delegated administration, or overlapping network namespaces become requirements.	No Change, Please be guided by the RFP
180	66	Point No. 7 Backup Solution of Appendix 1B	Backup Solution	Should be able to archive ALL workloads (VMs, DBs, Files) backup data by moving it to another disk target with different hardware using NFS/S3 protocols for long term retention and all the licenses for backup software and backup storage must be provided on day 1.	Clause repeated from #12. Request deletion of this clause as #12 provides additional clarity.	Please refer addendum for revised clause
181	67	Point No. 12 Backup Solution of Appendix 1B	Backup Solution	Proposed backup solution should support archiving the long term retention copies of ALL the workloads like VMs, DB, Files, etc on Long term Storage using NFS/S3 protocols and required software licenses must be provided on day 1.	Request specification change - Should be able to archive ALL workloads (VMs, DBs, Files) backup data by moving it to proposed/another disk target with different hardware using NFS/S3 protocols for long term retention and all the licenses for backup software and backup storage must be provided on day 1. Justification: Request to incorporate the change so that single and seamless solution can be provided to Bank. Also, ensures OEM's accountability on the solution design.	No Change, Please be guided by the RFP. The bidder shall size the proposed solution based on the backup, retention, long-term archival, recovery, and data-integrity requirements specified in the RFP. The bidder shall ensure adequate capacity and scalability to meet the stated requirements.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
182	68	Point No. 15 Backup Solution of Appendix 1B	Backup Solution	The following backup and retention policy to ensure data protection, recoverability, and compliance with long-term retention needs is complied: • Daily Incremental Backup – retained for 2 weeks in disk-based appliance/backup storage • Weekly Full Backup for all data types – Retained for 4 weeks in disk-based appliance/backup storage • Monthly Full Backups – Retained for 2 Months in the same appliance/backup storage *After the 2-month period, Monthly Full backups must be migrated to long-term backup storage, where they shall be retained for the entire duration of the contract. Backup Appliance / Backup Storage Requirements * Online Backup Storage/Appliance must retain backups for a minimum period of 2 months, with each Monthly backup being preserved during this duration. * All monthly backups taken during the contract period must also be stored on long-term storage for the entire duration of the contract. *All the data, logs, information & others must be backed up using the proposed backup and retrieval solution, in accordance with the defined backup policy and retention requirements. *Regularly test and verify the integrity of backed-up data and	Request Bank to provide the front end data size and the mix between Database, File and VM workloads.	Bidder and OEM to work together to design the solution
183	68	Point No. 17 Backup Solution of Appendix 1B	Backup Solution	Proposed backup solution must support software based de-duplication and shall be capable of taking backup of data and workloads (irrespective of the underlying storage OEM) and the solution shall support deduplicated backup copies for long-term retention. Based on policy backup software should be able to move deduplicated backup copy to a Long term storage automatically. The proposed backup solution shall support deduplicated backup targets across leading OEM storage systems and shall not be restricted on any specific OEM/vendor.	Request specification change - Proposed backup solution must support source side as well as target de-duplication and shall be capable of taking backup of data and workloads on the proposed backup appliance and the solution shall support deduplicated backup copies for long-term retention. Based on policy backup software should be able to move deduplicated backup copy to a Long term storage automatically. The proposed backup solution shall support deduplicated backup targets across leading OEM storage systems and shall not be restricted on any specific OEM/vendor. Justification: Request the change to allow a more efficient and open architecture.	Please be guided by RFP
184	68	Point No. 18 Backup Solution of Appendix 1B	Backup Solution	Proposed Disk Based Appliance/backup storage should have the capability to tier backup data to an external cloud storage (on premise / public cloud) and the required licenses must be provided on day 1. Proposed backup solution with storage/ appliance should have redundant components (Backup Storage - controllers, Power, fans etc. and Backup Appliance - Power, fans etc.), HA mechanism in place to avoid Single Point of Failure and should have minimum of 4x16/32 GB FC ports & 2x32G ports on each controller for Host connectivity. Proposed Backup Solution should have minimum 4x scalability of the current quoted capacity for future growth.	Request specification change - Proposed Disk Based Appliance/backup storage should have the capability to tier backup data to an external cloud storage (on premise / public cloud) and the required licenses must be provided on day 1. Proposed backup solution with storage/appliance should have redundant components (Backup Storage - controllers, Power, fans etc. and Backup Appliance - Power, fans etc.), to avoid Single Point of Failure and should have minimum of 4x10/25 GbE network ports & 4 x 32G FC ports on each controller for Host connectivity. Proposed Backup Solution should have scalable design for future growth. Justification: We recommend that the backup solution design should allow backup and restore operations to be distributed according to performance and SLA requirements, while enabling replication between separate protection systems and, where applicable. It should also provide greater flexibility for capacity expansion, maintenance, and future growth.	Please refer addendum for revised clause
185	69	Point No. 20 Backup Solution of Appendix 1B	Backup Solution	The proposed appliance/backup storage must ensure that all scheduled backups complete within an 8-hour backup window, with data protected via RAID 6 (or equivalent - providing 2 disk failure protection). Backup solution must support required technology and storage capacity to manage and compensate duplication across multiple pools, ensuring consistent performance and efficiency. Overheads in terms of memory, capacity, technology and IOPS to handle the bottleneck due to multiple deduplication pools should be factored and required documentation from the OEM is to be submitted along with the proposal.	Request specification change - The proposed appliance/backup storage must support a minimum of 25 TB/hr to ensure all scheduled backups complete within an 8-hour backup window, with data protected via RAID 6 (or equivalent - providing 2 disk failure protection). Backup solution must support required technology and storage capacity to manage and compensate duplication across multiple pools, ensuring consistent performance and efficiency. Overheads in terms of memory, capacity, technology and IOPS to handle the bottleneck due to multiple deduplication pools should be factored and Bidder must provide a sizing certificate showcasing this sizing consideration on the OEM's letter head with seal and sign from the authorized signatory. Justification: Request Bank to incorporate a minimum performance criteria as all Backup Storage architectures are different, capacity based sizing of the backup solution will not help Bank achieve performance outcomes.	No Change, Please be guided by the RFP
186		Backup Solution of Appendix 1B	New Point - Backup Solution		OEM & SI must ensure & implement backup solution in such a way that if Backups could be wrongfully expired and eventually deleted by tampered system clocks through a compromised NTP server. In this case, the local system clock would sync up based on the hacked NTP clock. This will minimize the systems clock tampering by an option which allows the security officer to set an allowed limit for the time drift between local system clock & NTP server. The proposed purpose-built backup appliance must have security feature which should protect against NTP hacking/compromise in case of Ransomware or Cyber-Attacks. Justification: Request Bank to incorporate this feature functionality which will enable backup data security during ransomware & cyber attacks.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
187		Backup Solution of Appendix 1B	New Point - Backup Solution		The backup solution shall provide security and cyber-resilience features including multi-factor authentication (MFA), data immutability / retention lock, and support for cyber recovery / isolated recovery workflows. Justification: Request Bank to incorporate this feature functionality which will provide multi factor authentication & enable stringent backup data security during ransomware & cyber attacks.	No Change, Please be guided by the RFP
188	89	7.18 IT Infrastructure requirements of RFP	Point No. 3	The proposed hardware infrastructure should be of the latest production available infrastructure not older than 2025.	Request specification change to - The proposed hardware infrastructure should not have End of service during the contract period Justification: Multiple products needs to service Govt RFP where higher shelf life is sought and hence we request bank to ask for service support for the contract period as this will ensure bank is covered from OEM side instead of restricting models with the hardware launch date	Please refer addendum for revised clause.
189	90	7.18 IT Infrastructure requirements of RFP	Point No. 19	Bidder can consider logical separation/ Virtualization for production and non-production environment at compute and storage level for respective Environments.	Point No. 8 of Pg no. 91 mentions that - The production and non-production environment should be physically separated to meet the requirement of the bank. Bank to suggest which one should be followed? Justification: Both the points are contradictory and requesting bank to clear out the point for sizing the hardware	Both Physical or Logical separation can be followed as per the Bidder proposed architecture
190	91	7.18.1 Compute Infrastructure of RFP	Point No. 8	The production and non-production environment should be physically separated to meet the requirement of the bank.	Point No. 19 of Pg No. 90 mentions that - Bidder can consider logical separation/ Virtualization for production and non-production environment at compute and storage level for respective Environments. Bank to suggest which one should be followed? Justification: Both the points are contradictory and requesting bank to clear out the point for sizing the hardware	Please refer addendum for the revised clause
191	98	8 CONTRACT PERIOD of RFP	4th Para	The pricing applicable during the extension period shall be mutually agreed and shall not exceed 120% of last year's AMC/ATS/Facility management rates quoted by the Selected Bidder.	Request specification change to - The pricing applicable during the extension period shall be mutually agreed % of last year's AMC/ATS/Facility management rates quoted by the Selected Bidder. Justification: Request Bank to remove the 120% capping as the future pricing can not be fixed at the bid submission.	No Change, Please be guided by the RFP
192	63	x86 Server of Appendix 1B	Internal Storage Point No. 5	The Server hardware RAID controller should support the following configurations RAID 0, 1, 5, 6, 10, 50, and 60. The raid controller should have minimum 4GB NV cache or higher	The Server hardware RAID controller should support the following configurations RAID 0, 1, 5, 6, 10, 50, and 60. The raid controller should have minimum 8GB NV cache or higher Justification: Kindly ask for 8GB NV cache instead of the minimum 4GB NV cache as it will ensure the proposed solution provides additional write caching headroom, improved performance under heavy I/O workloads, and better resilience for larger storage configurations and future expansion requirements.	No Change, Please be guided by the RFP
193	40	APPENDIX 1A Functional Compliance Sheet (Solutions)	NDR - Point No 7	Security Certification: The offered Packet Capture Application Platform/Product series shall have obtained cPP or EAL 4, or SOC2 or ISO Certificate of Common Criteria.	Please also include equivalent internationally recognized certifications covering quality management and information security management, such as ISO 9001 and ISO/IEC 27001. Request: Kindly confirm acceptance of such equivalent certifications.	Please refer addendum for the revised clause
194	40	APPENDIX 1A Functional Compliance Sheet (Solutions)	NDR - Point No 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high- availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	The RFP specifies the requirement for an on-premises deployment of the NDR solution. However, this clause mandates a cloud-native SaaS console with an Active-Active cloud architecture across multiple availability zones, which is only applicable to a cloud-based deployment model. Kindly delete this clause, as the requirement is for an on-premises NDR deployment and not a cloud/SaaS-based deployment.	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
195	75	Threat Intelligence Feed	7	The portal must provide IoC lookups (reputation & analysis). This capability should give insights to understand how malware files act and communicate. The TI tool should detonates files in virtual controlled environments to trace their activities and communications, producing detailed reports including opened, created and written files, created mutexes, registry keys set, contacted domains, URL lookups, etc. This execution activity should be indexed in a faceted fashion in order to allow for instantaneous lookups.	Changes Require: The portal must provide IoC lookups (reputation & analysis). This capability should give insights to understand how malware files act and communicate. The TI tool should detonates files in virtual controlled environments to trace their activities and communications, producing detailed summary including opened, created and written files, entropy map, registry keys set, contacted domains, URL lookups, etc. TI portal must have similarity, attribution and sandbox engine. This execution activity should be indexed in a faceted fashion in order to allow for instantaneous lookups. Justification: This is a globally established and recognized industry practice, so the requirement is technology-neutral and increases competition. An entropy map is a standard malware analysis indicator used to detect packing, encryption, and obfuscation within a file, and is essential for accurately identifying evasive malware that simple static reports may miss. Renaming 'detailed reports' to 'detailed summary' keeps the deliverable actionable and consumable for analysts without diluting the technical depth already listed. The specifications for the Threat Intelligence Platform and Threat Intelligence Feeds are closely interrelated, and no specific feeds have been defined under the Feed requirements. However, clauses related to Dark Web Monitoring, Brand Monitoring, ASM, etc. appear to overlap with capabilities	Please refer addendum for revised clause
196	76	Threat Intelligence Feed	12	The provider must cover Categorized threat lists for Ransomware & Malicious network infrastructure which will help to readily download and integrate actionable threat intelligence focused on specific threat types into their security tools.	Changes Require: The provider must cover network infrastructure which will help to readily download and integrate actionable threat intelligence focused on threats into their security tools. Justification: Restricting the clause to 'Ransomware' and 'specific threat types' unnecessarily narrows the scope and could disqualify capable vendors whose network infrastructure intelligence covers a broader range of malicious activity (e.g., C2 infrastructure, botnets, malware distribution, phishing infrastructure) beyond ransomware alone. Broadening the language to 'threats' in general keeps the requirement outcome-based and vendor-neutral, ensures comprehensive threat coverage rather than a single threat category, and allows fair participation by TI providers with wide-spectrum network infrastructure feeds.	Please refer addendum for revised clause
197	76	Threat Intelligence Feed	13	TI portal must have capability to search that allows users to ask natural language questions to get a generative AI-powered/AI-driven overview on their question	Changes Require: TI portal must have capability to get AI-generated summary of threat lookups that enable user to get more insights on the threat lookup. Justification: Mandating a specific interaction pattern (natural-language question and answer) prescribes a particular user-interface design rather than the underlying capability the organization actually needs. Not all leading TI platforms implement a conversational NLP search bar, even though most offer AI/GenAI-generated summaries and insights on indicators. Rephrasing the clause to require an 'AI-generated summary of threat lookups' keeps the intent (AI-driven, faster analyst insight) intact while making the requirement outcome-based and technology-neutral, ensuring wider and fairer vendor participation.	Please refer addendum for revised clause
198	76	Threat Intelligence Feed	14	TI provider must have capability to create YARA rules against URLs, domains and IP addresses and hunt for new network indicators that match certain metadata.	Changes Require: TI provider must have capability to investigate against URLs, domains and IP addresses and identify related network indicators that match certain metadata. Justification: YARA is a pattern-matching language designed primarily for identifying and classifying malware samples/files based on binary or textual patterns; it is not the conventional or appropriate mechanism for correlating or hunting network indicators such as URLs, domains, and IP addresses. Retaining 'create YARA rules' for this purpose is technically inaccurate and would unfairly disqualify TI providers that use other proven techniques (e.g., graph-based/relationship-based indicator correlation) to achieve the same investigative outcome. The revised wording ('investigate... and identify related network indicators') preserves the functional requirement, i.e. the ability to hunt for and pivot to related network indicators, while removing an overly prescriptive and technically inappropriate implementation detail.	Please refer addendum for revised claue
199	76	Threat Intelligence Feed	15	Threat intelligence provider must provide the relationships graph to understands the relationship between files, URLs, domains, IP addresses and other items encountered in an ongoing investigation (threat actors, campaigns, malware families, etc.). With it, TI analyst can pivot intelligently over any of the malware artifacts in your graph and synthesize your findings into a threat map.	Changes Require: Threat intelligence provider must provide the relationships graph to understands the relationship between files, URLs, domains, IP addresses and other items encountered in an ongoing investigation. With it, TI analyst can pivot intelligently over any of the malware artifacts in your graph and synthesize your findings into a threat map. Justification: The parenthetical examples (threat actors, campaigns, malware families) are illustrative only and already implicitly covered under 'other items encountered in an ongoing investigation.' Removing them avoids an unintentionally restrictive reading of the clause (i.e., limiting the relationship graph strictly to the listed entity types) and keeps the requirement focused on the core capability, understanding relationships between files, URLs, domains, IP addresses, and related investigative artifacts, without narrowing the scope of the graphing/pivoting engine.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
200	76	Threat Intelligence Feed	16	The provider must provide the curated Strategic Reporting generated by threat intelligence analysts in the following areas: a) Industry: Reports on threats specific to an industry vertical, considering various adversary motivations. b) Region / Country profile: Reports on threats targeting a particular country or geographic region, across different adversary motivations. c) Trends & Forecasting: Analysis of threat actor tactics, trends, and types of threat activity, potentially including historical reviews and predictions. d) Executive Perspective: Analysis about cyber threats relevant to events or business circumstances, geared toward a strategic leadership audience. This report type also includes Intelligence-at-a-Glance reports, which provide a weekly snapshot into newly produced reports, blogs, webinars; as well as some insight into customer interests based on top search terms and most read reports.	Changes Require: The provider must provide the curated Strategic Reporting generated by threat intelligence analysts in the following areas: a) Industry: Reports on threats specific to an industry vertical, considering various adversary motivations. b) Region / Country profile: Reports on threats targeting a particular country or geographic region, across different adversary motivations. c) Trends & Forecasting: Analysis of threat actor tactics, trends, and types of threat activity, potentially including historical reviews or predictions. d) Executive Perspective: Analysis about cyber threats relevant to events or business circumstances, geared toward a strategic leadership audience. This report type also includes Executive Summary reports, which provide techniques, tactics and procedures. Justification: The requirement is reworded from a vendor-specific product name ('Intelligence-at-a-Glance reports', tied to a particular provider's proprietary report format covering blogs, webinars, and search-term trends) to a content/outcome-based requirement ('Executive Summary reports... providing techniques, tactics and procedures'). This change makes the specification vendor-neutral and prevents the clause from being interpreted as favoring a single OEM's named product. It retains	Please refer addendum for revised clause
201	76	Threat Intelligence Feed	17	The provider must provide curated details on various aspects of adversary activities, with a focus on their methods and behaviors. Including: a) Actor Profile: In-depth look into a specific threat actor's tactics, techniques, and procedures. b) TTP Deep Dives: Detailed analysis into a threat actor and the tactics, techniques, and procedures (TTPs) they use to achieve specific goals. c) Event Coverage / Implication: Analysis on the implications of a recent event or campaign conducted by a threat actor. d) Malware Profile: Technical analysis of a representative sample of a code family. This report type typically includes file characteristics, host- and network-based indicators, configuration information, and details of code execution.	Changes Require: The provider must provide curated details on various aspects of adversary activities, with a focus on their methods and behaviors. Including: a) Actor Profile: In-depth look into a specific threat actor's tactics, techniques, and procedures. b) TTP Deep Dives: Detailed analysis into a threat actor and the tactics, techniques, and procedures (TTPs) they use to achieve specific goals. c) Event Coverage / Implication: Analysis on the implications of a recent event or campaign conducted by a threat actor. d) Malware Profile: Technical analysis of a representative sample of a code family. This report type typically includes capabilities, TTP details, expert analysis and references. Justification: The original clause lists very specific technical fields (file characteristics, host-/network-based indicators, configuration information, code-execution details) that may not map exactly to how every TI provider structures a Malware Profile report, even though the underlying analytical depth is equivalent. Rewording to outcome-based descriptors (capabilities, TTPs, expert analysis, references) preserves the requirement for a comprehensive, expert-driven technical malware profile while avoiding disqualification of vendors whose reports are equally rigorous but organized differently, thereby ensuring wider and fairer participation without	Please refer addendum for revised clause
202	109	10.2 Eligibility Evaluation Criteria	12	The bidder shall submit a self-declaration confirming that, during the last three (3) years preceding the date of publication of this RFP, no contract, Purchase Order, or award issued by Punjab & Sind Bank (PSB) to the bidder has been cancelled, terminated, rescinded, or revoked due to non-performance, breach of obligations, or failure to comply with post-award requirements.	Bidder's Query: The RFP already contains a clause restricting participation of bidders who have been blacklisted/debarred by Regulators, Government bodies, Banks, or Financial Institutions during the last three years. In view of the existing debarment provision, the above clause may be considered overlapping and restrictive, as contractual cancellation/termination may occur due to various circumstances and does not necessarily imply debarment or unsuitability for the present tender. Request: We request the Bank to kindly delete the above clause to facilitate wider participation, healthy competition, and a level playing field for all eligible bidders.	No Change, Please be guided by the RFP
203	103	10.2	12	The bidder should have a minimum average turnover of INR 500 crore per annum in India during the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth.	Pls amend the minimum average turnover of INR 300 Crore per annum in india during last 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth for maximum competion.	No Change, Please be guided by the RFP
204	103	10.2	12	The bidder should have a minimum average turnover of INR 500 crore per annum in India during the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth.	Kindly clarify whether Medium Enterprises registered under Udyam are eligible for turnover relaxation.	No Change, Please be guided by the RFP
205	103	10.2	12	Bidder must have at least enrolled manpower (on bidder's payroll) of 100 experienced employees skilled in areas of Cyber security.	Bidder must have at least enrolled manpower (on bidder's payroll) of 100 experienced employees skilled in areas of Cyber security/IT Experts/Telecom Engineers	No Change, Please be guided by the RFP
206	103	10.2	12	The Bidder must have successfully supplied, installed and maintained (or under maintenance) SIEM Solution of minimum 20000 EPS / 0.86 TB per day in one PSU/ PSE/ Government Organizations / BFSI/Telecom provider in India in last 5 years	Pls amend-The Bidder must have successfully supplied, installed and maintained (or under maintenance) SIEM Solution of minimum 20000 EPS / 0.86 TB per day or Managed Telecom Services(OFC Maintenace)/O&M Enode B/BTS in one PSU/ PSE/ Government Organizations / BFSI/Telecom provider in India in last 5 years	Please refer addendum for revised clause.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
207	105	10.2	12	Bidder should have supplied, installed and maintained (or under maintenance) any three (3) of the below solutions in any one PSU/PSE/ Government Organizations / BFSI/Telecom provider in India a. SOAR b. UEBA c. Extended Detection & response (XDR)/ Endpoint Detection & response (EDR) d. Network Detection & response (NDR)/Network Behaviour Anomaly Detection (NBAD) e. Threat Intelligence Platform f. Vulnerability Assessment/Vulnerability management g. Identity Threat Detection & response h. Decoy/Honeypot/Deception i. Application security testing tool (DAST or SAST) j. Cloud Security Posture Management (CSPM) k. Cloud-Native Application Protection Platform (CNAPP) l. Cloud Workload Protection Platform (CWPP) m. Continuous Threat Exposure Management (CTEM)	Pls include following services- a) Managed Services b) Data Center Hardware C) Wifi Implementation	Please refer addendum for the revised clause
208	20	6.1	Earnest Money Deposit (EMD)	Earnest Money Deposit (EMD)	Kindly clarify whether Medium Enterprises registered under Udyam are eligible for EMD exemption. If yes, please specify the relevant category/provision under which such exemption can be claimed.	No Change, Please be guided by the RFP
209	109-128	10.2	General Note (m)	Experience must be showcased separately for each solution category, with clear evidence that each solution has been deployed as a standalone solution and not merely as a feature or component of another solution.	Several leading platforms natively deliver multiple solution categories within a single licensed product (for example SIEM with integrated UEBA, or a cloud security platform covering CSPM, CNAPP and CWPP). Request the Bank to confirm that where a single OEM platform is licensed and delivered for multiple categories, the credentials submitted for that platform will be accepted against each applicable category, and that technical marks under Section 10.3 will be awarded per category.	Yes. Where a single OEM natively provides multiple solution categories, the same credentials may be considered for each applicable category, provided the submitted documents clearly establish the required scope for each category.
210	101-102	10.2	Criterion 5 - MAF	MAF should be submitted from the OEMs of all 14 solutions and all 9 services.	Where a single OEM platform covers multiple solution or service categories, request the Bank to confirm that one MAF from that OEM, listing all applicable categories, is sufficient.	MAF should be mentioned all the details explicitly for all the solutions or services
211	250	16.19	Annexure 19 - Stack Confirmation Sheet	Stack Confirmation Sheet - Undertaking for Proposed OEM Products.	Where one licensed platform delivers multiple solution categories, request the Bank to confirm whether it should be declared once against all applicable categories, or repeated as separate line items in Annexure 19 and in Appendix 2 - Commercial Bill of Material.	No Change, Please be guided by the RFP
212	101	10.2	Criterion 4 - Turnover	The bidder should have a minimum average turnover of INR 500 crore per annum in India during the past 3 financial years along with positive net worth.	Request the Bank to confirm that this refers to the turnover of the bidding Indian legal entity, and to clarify whether the combined turnover of the bidder's group entities registered in India may be considered where supported by audited financial statements.	No Change, Please be guided by the RFP
213	129	10.3	Criterion 2 - Bidder SIEM experience	The Bidder must have successfully supplied, implemented, and maintained a SIEM Solution in at least one PSU/PSE, Government Organisation, BFSI organisation or Telecom provider, scored across EPS / TB per day bands.	Request the Bank to confirm whether SIEM deployments supplied, implemented and maintained by the bidder outside India are eligible for scoring, or whether only India deployments will be considered.	No Change, Please be guided by the RFP
214	110-123	10.2	Criteria 19 to 22 - OEM credentials	The proposed OEM solution should have been implemented in at least one client in India, for each listed solution and service.	Several of the specified categories have a limited number of India references. Request the Bank to confirm whether global deployments of the proposed OEM solution, confirmed by the OEM, will be accepted where India references are not available.	No Change, Please be guided by the RFP
215	103-108	10.2	Criteria 7 and 8 - Credential evidence	Bidder to submit Purchase Order / Work Order / Contract, plus a client-issued supporting document, plus a self-declaration.	Many BFSI, PSU and Government clients do not permit release of purchase orders or capacity details due to confidentiality obligations. Request the Bank to accept a client-issued credential or experience certificate together with bidder and OEM self-declarations, where the purchase order cannot be shared.	No Change, Please be guided by the RFP
216	159	14.1	Assignment & Subcontracting	The selected bidder shall not subcontract or permit anyone to perform any of the work (excluding Proposed OEM personnel). All bidder's personnel proposed for the bank shall be on bidder's payroll.	Request the Bank to confirm that (a) OEM implementation and subject matter expert resources are excluded from this restriction as stated in the clause, and (b) resources employed by the bidder's affiliate or group entities registered in India may be deployed, subject to prior Bank approval.	No Change, Please be guided by the RFP
217	128	10.2	General Note - Mutual exclusivity	A bidder declared successful in either the NextGen SOC RFP or the IT Security solution (Part A / Part B and Firewall) and services RFP shall be deemed ineligible for award in the other.	Request the Bank to clarify the sequence in which the two RFPs will be evaluated and awarded, and whether a bidder qualifying in both will be given an opportunity to indicate a preference prior to commercial bid opening.	The two RFPs shall be evaluated and awarded independently as per the respective provisions of the RFPs. The RFP for which the award is finalized first shall determine the bidder's eligibility for the subsequent RFP. Accordingly, a bidder declared successful and awarded the contract under either RFP shall be deemed ineligible for award under the other RFP. No separate opportunity shall be provided to a bidder to indicate a preference prior to the opening of the commercial bids.
218	7	1	Key Information - EMD	Security Deposit / Earnest Money Deposit: Rs. 4.25 Crore.	Request the Bank to confirm that a Bank Guarantee in the format prescribed at Annexure 15 is acceptable in lieu of EMD, and to confirm the required validity and claim period of such Bank Guarantee.	No Change, Please be guided by the RFP
219	7	1	Key Information - Bid submission	Last Date and Time for submission of Bids: As per GeM Portal.	The bid requires Manufacturer Authorisation Forms, OEM self-declarations and client-issued credential evidence from 23 OEMs. Request the Bank to confirm the bid submission date and to consider allowing a minimum of three weeks from the date of publication of pre-bid replies and corrigendum.	Please refer addendum for the revised clause
220	21	6.11	Performance Bank Guarantee	Performance Bank Guarantee: 5% of Project Cost.	Request the Bank to confirm the basis of 'Project Cost' - whether it means the total contract value including AMC, ATS and Facility Management for the full contract period, or the one-time supply and implementation value.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
221	163	14.14	Make in India	Make in India provisions and Annexure 7 - Minimum Local Content Certification.	Request the Bank to confirm the applicable minimum local content percentage and whether the purchase preference for Class-I and Class-II local suppliers applies to this procurement, given that most of the specified solution OEMs are foreign manufacturers.	No Change, Please be guided by the RFP
222	165	14.21	Limitation of Liability	Limitation of Liability.	Request the Bank to confirm that the bidder's aggregate liability under the contract is capped at the total contract value, and that indirect, incidental and consequential losses, including loss of profit and loss of business, are excluded.	The At-Risk Amount is a contractual performance mechanism and shall be withheld/adjusted in accordance with the applicable performance requirements specified in the RFP. It shall not automatically be treated as an additional penalty or Liquidated Damages (LD). Any withholding, adjustment or recovery under the At-Risk Amount shall be accounted for within the overall 10% penalty/LD cap specified in Section 13.2 and shall not be over and above such cap.
223	146, 157-158	13.1, 13.2, 13.3	SLA penalties and At-Risk Amount	Availability penalty of 1% of Monthly Maintenance Cost for every 0.05% drop, rising to 100% of Monthly Maintenance Cost below 90%. Total LD and SLA penalties capped at 10% of overall contract value. Monthly At-Risk Amount of 15% of estimated monthly payout.	Request the Bank to confirm that all service level penalties, including the availability penalty, are counted within the overall cap of 10% of total contract value stated in Section 13.2, and to clarify how the monthly At-Risk Amount operates alongside that cap.	The At-Risk Amount is a contractual performance mechanism and shall be withheld/adjusted in accordance with the applicable performance requirements specified in the RFP. It shall not automatically be treated as an additional penalty or Liquidated Damages (LD). Any withholding, adjustment or recovery under the At-Risk Amount shall be accounted for within the overall 10% penalty/LD cap specified in Section 13.2 and shall not be over and above such cap.
224	95, 98	7.19.2, 9	Transition and project timelines	Transition Management refers to takeover of existing solutions on an as-is / where-is basis. Section 9 states an overall implementation period of 5 months from T0 (date of acceptance of PO).	Request the Bank to confirm the expected T0 date and to clarify how the transition takeover date aligns with the 5-month implementation window, including whether transition activities run in parallel with implementation.	No Change, Please be guided by the RFP
225	26	7.1	Scope and Objectives	The implementation of each proposed solution shall be performed by the respective OEM. Upon successful implementation, the respective OEM shall provide a certificate confirming that the solution has been deployed by the OEM and complies with all functional and technical requirements.	As System Integrator, the bidder has established capability to design, build and implement these solutions and can bundle professional services within its offer. Request the Bank to confirm whether implementation must be performed exclusively by OEM resources, or whether the bidder may implement using its own certified resources under OEM supervision and governance, with the OEM issuing the completion certificate confirming alignment to the RFP and SRS.	No Change, Please be guided by the RFP. Refer Section 7.6 OEM Responsibilities
226	27	7.1	Current SOC environment	Migration from the Bank's current SOC to the NextGen SOC.	To enable accurate sizing, transition planning and effort estimation, request the Bank to share: (a) current SIEM OEM and version; (b) capabilities currently in use such as SIEM, SOAR and Threat Intelligence; (c) number of integrated log sources and devices; (d) peak and average EPS and daily data volume; (e) average monthly alert and incident volumes; (f) current ITSM platform and whether automated ticketing integration exists; (g) number of use cases and correlation rules configured and whether they are mapped to MITRE ATT&CK.	Details shall be shared be with successful bidder
227	41	7.3.1.2	SIEM - EPS measurement	Total 50,000 sustainable EPS / 2.06 TB per day of data ingestion from the outset, scalable to 75,000 sustainable EPS / 3.09 TB per day at DC and DR.	Request the Bank to confirm the EPS measurement point - whether EPS is measured before or after filtering, de-duplication and aggregation at the broker, aggregator or collector layer, and whether sizing based on post-reduction ingestion volume will be accepted.	Refer Section 7.3.1.2 SIEM Data ingestion and EPS measurement Please refer addendum for the revised clause The bidder shall be provided with an on-premise/onsite measurement, collection or monitoring component capable of measuring and reporting the volume of logs/events forwarded towards the SIEM
228	256-261	Annexure 21	Sizing and Volumetrics	Annexure 21 sets out solution-wise volumetrics and a tentative count of current IT and security infrastructure.	Request the Bank to share the current log volumes (EPS and TB per day) and the confirmed asset inventory by category before bid submission, to enable accurate sizing of SIEM, UEBA, storage and backup infrastructure.	Refer Section 7.3.1.2 SIEM Data ingestion and EPS measurement The bidder shall be provided with an on-premise/onsite measurement, collection or monitoring component capable of measuring and reporting the volume of logs/events forwarded towards the SIEM
229	47	7.3.8	Vulnerability Assessment	The VA solution is to be deployed On-Premises, Standalone at DC and Standalone at DR. Minimum number of IPs: 4,000.	Request the Bank to confirm whether authenticated scanning of all assets, including cloud workloads and databases, is within scope, and to share the split between internal and external IPs to enable accurate sizing.	No Change, Please be guided by the RFP
230	Appendix 1A, 40	7.3.5	NDR - interface details	Network Detection and Response, throughput requirement of 10 Gbps.	Request the Bank to confirm the physical interface type and speed that will be provided for the uplink to the NDR sensors at DC and DR, and whether TAP or SPAN based traffic feeds will be made available.	Bank will provide the Core Switch supporting 10/25 G Ports. Bidder should bring the required SFP/SFP+
231	54-58	7.4	Offsite Services	All nine offsite services are to be delivered under a Managed Service model.	Request the Bank to confirm whether a single OEM or service provider may deliver multiple services (for example Breach and Attack Simulation, Continuous Automated Red Teaming and Attack Surface Management from one provider), or whether a separate provider is required for each service.	No Change, Please be guided by the RFP
232	68	7.7	On-cloud OEM Responsibilities	The proposed solution shall support customer-managed encryption key arrangements.	Request the Bank to clarify whether Bring Your Own Key using a Bank-managed external KMS or HSM is required, or whether CSP-native or OEM-native key management with customer-managed keys is acceptable.	Currently, KMS is not in place, and the Bank is sourcing the same through a separate RFP. Until the KMS solution is procured and implemented, the OEM-native or CSP-native KMS shall be provided as part of the proposed solution.
233	43, 46, 48, 51-54	7.3.2.2, 7.3.7.2, 7.3.9.2, 7.3.11.2, 7.3.12.2, 7.3.13.2	Key Deliverables - backup and restoration	Backup, retention, restoration and knowledge transfer requirements repeated across solution-wise Key Deliverables, including restoration of data from backup for forensic and regulatory purposes without additional cost.	For solutions delivered as SaaS, configuration and operational data reside on the OEM platform. Request the Bank to clarify its expectation - specifically whether periodic export of configuration, rules, reports and operational data to the Bank's backup infrastructure at DC and DR is required, and if so the expected frequency, format and retention period.	No Change, Please be guided by the RFP Refer Section7.2.4.3 Storage and other Requirement
234	43, 54	7.3.3.2, 7.3.14.2	Key Deliverables - reporting	Reports covering user and entity risk, anomalies, behavioural trends, privileged user activities and detection effectiveness; Periodic Exposure Review and Risk Trend Report.	Request the Bank to share indicative report templates, the expected reporting frequency and the intended recipients, to enable the bidder to size the reporting and analytics effort accurately.	Details shall be shared with the successful bidder

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
235	29-35	7.2.1, 7.2.3, 7.2.4	Deployment model and HA requirement	Bank Location: Broker / Aggregator / Collector: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Cloud (SaaS): HA deployment aligned with the SLA, RTO and RPO. Management Console: deployed at both Primary and Secondary sites.	Several of the specified solutions are available only as multi-tenant SaaS, where the vendor operates the platform, console, resiliency and disaster recovery, and only lightweight collection or broker components are deployed in the Bank's environment. Request the Bank to confirm the following principle, applicable to all clauses listed in the annexed sheet 'Annex A - SaaS Clause List': (a) Bank-side N+N Active-Active HA requirements apply only to on-premises components such as brokers, collectors, connectors and sensors; (b) platform availability, resiliency, disaster recovery, RTO and RPO for vendor-hosted components are met through the OEM's cloud-native architecture and published SLA; (c) the requirement for a management console at both primary and secondary sites is met by a single SaaS console securely accessible from both Bank sites.	Please refer addendum for the revised clause
236	35	7.2.4.1	Deployment Pattern - point g (ITDR)	The ITDR solution shall be deployed On-Premises, with N+N Active-Active configuration at both the Bank's DC and DR.	Leading Identity Threat Detection and Response capabilities are delivered as SaaS with agent or sensor based collection. Request the Bank to permit a SaaS or hybrid ITDR deployment, with Bank-side collection components deployed in high availability at DC and DR.	Please be refer addendum for revised clause
237	35	7.2.4.1	Deployment Pattern - point d (NDR)	The NDR solution shall be deployed On-Premises within the Bank's DC and DR, with the required brokers, aggregators, collectors and/or enforcement components configured in N+N Active-Active configuration at both sites.	Request the Bank to permit a hybrid deployment with an OEM-managed console, and on-premises sensors and collectors deployed in N+N Active-Active or Active-Passive configuration at DC and DR.	Please refer addendum for the revised clause
238	41	7.3.1.1	SIEM - Modules, Architecture and Deployment, point 7	All SIEM components, including collectors, ingestion nodes, correlation engines and processing nodes, are to be deployed in the prescribed HA architecture irrespective of whether they are at the Bank's DC, DR, CSP Primary Site or CSP Secondary Site.	For a SaaS-delivered SIEM, ingestion, correlation and processing are operated by the OEM under its published availability SLA and are not exposed for customer-side HA configuration. Request the Bank to confirm that this requirement is met through the OEM's cloud-native high availability, with the on-premises broker or collector components deployed in high availability across DC and DR.	No Change, Please be guided by the RFP. Maintaining HA, if deployed on-premise, and Uptime Compliance (for On-cloud/SaaS).
239	Appendix 1A, 2-11	Cloud CSP	Points 3 and 18	The proposed cloud infrastructure should be deployed in High Availability mode (N+N) at both primary and secondary site. The cloud infrastructure should have presence in at least 2 cities in India in different seismic zones.	For multi-tenant SaaS platforms the vendor does not expose region or availability zone architecture for customer configuration. Request the Bank to accept, as an alternative, either presence in at least two India locations in different seismic zones, or a committed platform availability of 99.99% from a single India region backed by the OEM's published SLA.	Please refer addendum for revised clause
240	Appendix 1A, 2-11	Cloud CSP	Points 27, 32 to 37, 39 to 47, 50, 57, 58, 60	Requirements covering virtual environment security, encryption and key management, monitoring, data segregation, network segmentation, identity and access management, secure SDLC, business continuity and disaster recovery, change and configuration management, and secure configuration baselines.	For pure SaaS platforms these controls are designed, implemented and operated by the OEM within its own platform rather than configured by the Bank or the bidder. Request the Bank to confirm that compliance will be evidenced through the OEM's independent third-party attestations and certifications, including SOC 2 Type II, ISO 27001, ISO 27017, ISO 27018 and CSA STAR, together with the OEM's published security documentation, in place of Bank-specific configuration evidence.	Please refer addendum for the revised clause
241	Appendix 1A, 2-11	Cloud CSP	Points 38, 41.4 and 41.5	Reverse data shifting on completion or termination of contract; transferability of cloud outsourced services; the format and manner in which data is to be returned to the Bank.	Request the Bank to confirm that this requirement is met through the OEM's documented data export capability in standard machine-readable formats at the end of the contract, delivered within a mutually agreed timeline and supported by the bidder.	No Change, Please be guided by the RFP
242	Appendix 1A, 2-11	Cloud CSP	Point 23	The proposed solution should also have Service level commitments for virus detection and blocking, spam effectiveness, false positives as well as email delivery.	This requirement appears to relate to an email security solution and does not appear applicable to the solutions in scope under this RFP. Request the Bank to confirm its applicability or to remove it from the cloud requirements for this procurement.	Please refer addendum for revised clause
243	32	7.2.2	Services - point 3 (ASM)	Attack Surface Management: Managed Service, continuous 24x7 monitoring, weekly discovery and update, monthly reporting.	Request the Bank to confirm whether a dedicated Attack Surface Management platform and service is required, or whether ASM capability delivered as part of a broader exposure management platform is acceptable, provided the prescribed discovery, monitoring and reporting frequencies are met.	Bidder to propose the Offiste Services complying with the specification mentioned in the RFP.
244	Appendix 1A, 23	SIEM	Point 36	The proposed solution must come with out-of-the-box / customized day 1 support, integration, dashboards, reports and rules providing operational visibility into large-scale CentOS, Windows, Unix and Linux environments machine data: syslog, metrics and configuration files.	Request amendment to read: '...operational visibility into large-scale CentOS, Windows and Linux environments machine data: syslog, metrics and configuration files.' Native Unix support is available with a limited set of vendors and its removal will widen participation without affecting the Bank's requirement.	No Change, Please be guided by the RFP
245	Appendix 1A, 24	SIEM	Point 59	The proposed solution machine learning capabilities must allow addition or have inbuilt feature of custom machine learning algorithms from popular open-source libraries like NLP, Python etc.	Request amendment to read: 'The proposed solution must support custom machine learning models through a bring-your-own-machine-learning framework, allowing the Bank's analysts and data scientists to run bespoke analytics on the security data retained within the platform.'	No Change, Please be guided by the RFP
246	Appendix 1A, 37	XDR	Point 43	The proposed solution must include functionality to perform sandbox analysis of suspicious files, provided natively or through integration with a third-party sandbox from day 1. Sandboxing analysis should have no limit on the size or the quantity of agents sending the data.	Request amendment to read: 'The proposed solution must include functionality to perform sandbox analysis of suspicious files, provided either as a native capability or through seamless integration with a third-party sandboxing solution from day one.' Sandbox file size and submission limits are defined by the respective OEM and an unlimited commitment restricts participation.	Please refer addendum for revised Clause
247	Appendix 1A, 52-53	ITDR	Points 1.4, 2.15 and 3.7	1.4 --Requirements to present high-risk attack pathways to critical IT assets, 2.15 Identity Threat Detection controls should be able to automatically discover and flag hidden or shadow Tier 0 assets 3.7 Identity Threat Detection Solution should, as part of its forensic data collection process, include detailed attack path information, including the protocols leveraged during the attack.	Request amendment to a capability-based outcome: 'The solution shall provide identity risk context across assets, permissions and access relationships, and shall identify high-risk identities, excessive privileges and exposure paths to critical assets.' The prescribed feature-level wording is specific to a limited set of vendors.	Please refer addendum for revised Clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
248	Appendix 1A, 52	ITDR	Points 1.6, 2.3, 2.4 and 2.5	1.6 Identity Threat Detection Solution should must automatically prioritize and remediate the riskiest identities to preemptively cut off what attackers need (and expect to find) to move undetected within the network. 2.3 The ITDR solution shall identify and assess exposed, improperly stored, or compromised credentials associated with user, privileged, service, and administrative identities on endpoints 2.4Identity Threat Detection Solution should Identify, Misconfigured accounts, Legacy app accounts, Stale accounts, password policy violations, Kerberoastable credentials, unmanaged user accounts, unmanaged service accounts 2.5 "Identity Threat Detection Solution should Provide continuous monitoring and customizable, automated business rules to eliminate security policy violations, such as: • Stored credentials to sensitive assets • Local-admin accounts • Cached credentials stored in browsers, Windows and other systems"	Request amendment to: 'The solution shall continuously monitor identity posture and identify weak, exposed or compromised credentials, misconfigured and stale accounts, excessive privileges, Kerberoasting activity and policy violations across user, privileged, service and administrative identities, and shall support remediation workflows for identified risks.'	Please refer addendum for revised clause
249	Appendix 1A, 52	ITDR	Point 2.7	Identity Threat Detection Solution should be available through rack-mountable on-premise deployment.	Request amendment to read: '...available through rack-mountable on-premises deployment, or as a SaaS-delivered solution with on-premises collection components.' This aligns with the deployment clarification sought at Section C above.	Please refer addendum for revised clause
250	Appendix 1A, 52	ITDR	Point 2.9	Identity Threat Detection Solution should detect all types of attack vectors including but not limited to pre-attack reconnaissance, zero-day attacks, privilege escalation prevention, lateral movement and data theft.	Request amendment to read: 'The solution shall detect identity-based threats including directory reconnaissance, compromised accounts, privilege escalation, lateral movement and anomalous access, and shall provide identity context to support investigation of exposure and attack paths.' A commitment to detect all zero-day attack vectors cannot be substantiated by any vendor.	The Clause is applicable only to idendity related threat vector only.
251	Appendix 1A, 52	ITDR	Point 2.17	Identity Threat Detection Solution should be able to pull and analyze identity data from AD, Entra ID, identity stores and PAM systems.	Request amendment to read: 'The solution shall analyse identity data from supported identity sources, including Active Directory and Microsoft Entra ID, with integration to additional identity and privileged access platforms where supported by the OEM.'	Please refer addendum for revised clause
252	Appendix 1A, 52	ITDR	Points 3.4 and 3.5	3.4 Integration with compatible endpoint or extended detection solutions to capture screen recordings or screenshots during active attacker sessions, and with network detection solutions to collect PCAP data. 3.5 The Identity Threat Detection Solution should integrate with compatible network detection solution to support collection of PCAP data to support network-level visibility of the incident	Request amendment to read: 'The solution shall integrate with supported endpoint and network detection tooling to share identity, endpoint and network context for investigation and response, including forensic data collection where available.' Screen recording and PCAP capture during attacker sessions are vendor-specific capabilities.	Please refer addendum for revised clause
253	Appendix 1A, 53	ITDR	Point 3.9	Identity Threat Detection solution should detect an adversary's attempt to move laterally toward key assets using as many hosts (Windows, Mac or Linux) as possible without requiring a persistent agent.	Request amendment to read: '...using as many hosts (Windows, Mac or Linux) as possible, with or without a persistent agent.' Both agent-based and agentless detection approaches deliver the required outcome.	Please refer addendum for revised clause
254	Appendix 1A, 53	ITDR	Points 3.10 and 3.11	3.10 Identity Threat Detection Solution should collect user and computer information from Active Directory as part of its forensic data gathering to enhance context and assess risk exposure. detect at the earliest point in the attack, post initial compromise as the attacker is first attempting to move laterally and escalate privilege. 3.11 Identity Threat Detection Solution should collect user and computer data from Active Directory during forensic data gathering to improve context and evaluate risk exposure, while ensuring that all deception techniques remain hidden from legitimate users.	Request amendment to read: 'The solution shall collect and analyse identity data from Active Directory and other supported identity sources to provide context and assess risk exposure, and shall detect identity-based threats such as compromised accounts, privilege escalation, anomalous access and directory reconnaissance early in the attack path.' The requirement relating to deception techniques belongs to the Deception solution specification.	Please refer addendum for revised clause
255	Appendix 1A, 19	CTEM	Point 7	Each intelligence item should include metadata such as date, author, source, and pre-classification of raw data.	Request amendment to read: 'Each intelligence item shall include enriched context, source attribution and analysis metadata to support investigation and prioritisation.' Author-level attribution of raw intelligence is not published by all providers.	Please refer addendum for revised clause
256	Appendix 1A, 19	CTEM	Point 11	The solution / service should generate investigation reports for designated VIPs or other high-risk identities and assets, providing an overview of identified digital exposure and associated risk.	Request amendment to read: 'The solution shall provide risk context and investigation views for designated high-risk identities and assets, enabling analysts to assess digital exposure and associated risk.'	No Change, Please be guided by the RFP
257	Appendix 1A, 19	CTEM	Points 19 and 21	19 The solution should detect compromised credentials for employees and VIPs, exposed payment card information, and aggregate data from known breach databases in real time 21 The solution should support threat actor interaction via vendor analysts (e.g., engaging via dark web avatars) to gather additional intelligence	These are typically delivered through a dark web monitoring and threat intelligence managed service rather than as a platform feature of the exposure management tool. Request the Bank to confirm that these requirements may be met through the Dark Web Monitoring and Threat Intelligence services proposed under Section 7.4, rather than within the CTEM platform.	Please refer addendum for revised clause
258	Appendix 1A, 20	CTEM	Point 38	The solution should be deployed agentlessly, without requiring sensors or agents on endpoints, servers or network appliances.	Request amendment to read: 'The solution should be deployed agentlessly, or with lightweight sensors or agents where these improve discovery coverage and accuracy.'	Please refer addendum for revised clause
259	Appendix 1A, 81	ASM	Point 6	The visual representations should be downloadable in PDF, JPG, PNG and other generally used formats.	Request amendment to read: 'The solution shall support export of reports and data views in commonly used formats such as PDF, CSV, JSON or ZIP, appropriate to the workflow.'	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
260	Appendix 1A, 81	ASM	Points 8, 9 and 10	8 -- The solution shall provide information on vulnerabilities, misconfigurations, insecure configurations, obsolete or unsupported technologies, applications, services, URLs, ports, network components, systems, databases and other relevant infrastructure that are publicly exposed or otherwise identifiable through authorized discovery and assessment activities. 9 -- The solution should provide data/information on security flaws/ inherent vulnerabilities (allegedly) reported about the digital products exposed to the Internet (For example: internet banking, mobile applications) offered to the bank's customers, as leaked in public domain, or other forums 10 -- The solution shall identify and provide relevant information on potentially exposed sensitive information associated with the Bank, including source-code references, code snippets, API information, credentials, keys and other security-relevant information, where such information is identifiable through publicly available sources, external attack-surface intelligence or other authorized discovery mechanisms.	Request consolidation and amendment to read: 'The solution shall provide exposure information for the Bank's internet-facing assets, including vulnerabilities, misconfigurations, unsupported technologies, exposed services and ports, code weaknesses and exposed secrets, discovered through authorised external attack surface discovery and assessment.'	8 -- Please refer addendum for revised clause 9 -- No Change, please be guided by the RFP 10 -- Clause stands deleted
261	Appendix 1A, 54	Cloud Security (CSPM)	Point 4	The solution must provide cloud compliance scanning against industry benchmarks (e.g. CIS Benchmark for AWS / Azure / GCP / Meghdoot, AWS Well-Architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with ability to create custom standards and reports.	Request the Bank to confirm whether the Bank's workloads are hosted on Meghdoot, and if not, to remove Meghdoot from the required benchmark list, as coverage for it is not available across the leading CSPM platforms.	Please refer addendum for revised clause
262	Appendix 1A, 55	Cloud Security (CSPM)	Point 9 (sub point)	Automatic, in-product remediation via the Cloud Service Provider (CSP) API (1-click).	Request amendment to read: 'The solution shall support in-product remediation workflows, including automated actions and approval-based playbooks where configured by the Bank.' Fully automatic remediation without approval is generally not permitted under Bank change management controls.	Please refer addendum for revised clause
263	Appendix 1A, 56	Cloud Security (CSPM)	Point 25	The solution must provide a self-service portal for engineers, with admin-defined eligibility for users and groups based on role, scope and duration, approval workflow and audit logs.	This describes a just-in-time privileged access capability which is typically delivered by a PAM or IGA platform rather than a CSPM tool. Request amendment to read: 'The solution shall support granular role-based access control, approval workflows for privileged actions, and audit logging of access-related changes.'	Please refer addendum for revised clause.
264	Appendix 1A, 40	NDR	Point 9	Easy-to-manage, clientless platform that deploys quickly and involves minimal or no dependency on customization and management.	Request amendment to read: 'Easy-to-manage platform, whether client-based or clientless, that deploys quickly with minimal dependency on customization and ongoing management.'	Please refer addendum for revised clause
265	Appendix 1A, 40	NDR	Point 13	The proposed solution shall feature a cloud-native SaaS console with an underlying dashboard and administration interface operating in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead.	Request amendment to read: 'The proposed solution shall feature a customizable security console with dynamic role-based access control, accessible from both the Bank's primary and disaster recovery sites, with availability and resiliency in accordance with the applicable deployment model and SLA.'	Please refer addendum for the revised clause
266	23	SIEM / Functional Specification	23	Where a native parser or connector is unavailable, the proposed solution shall provide supported mechanisms, SDKs, APIs, templates, or configuration interfaces to develop and maintain custom integrations	For a recuced overall TCO and ensure the timely availability without any delay, please rephrase it to: OEM /OEM authorized partner to provide parsers for data ingestion for all the current data sources and their respective upgrades (in maximum 15 business days from data of intimation of the same) during the contract period. If any new data source is added during the contract period, the OEM will provide parsers for data ingestion in maximum 15 business days from data of intimation of the same, without dependency of the bidder.	No Change, Please be guided by the RFP
267	28	SIEM / Incident Response	131	The proposed cloud-delivered solution shall provide secure multi-tenant architecture with appropriate logical tenant isolation, encryption in transit and at rest, secure authentication, MFA, granular RBAC, audit logging and protection of Bank security data in accordance with the approved service architecture, security controls and SLA.	Why there is a need for multi-tennacy, this is specially required in a service provider environment needing multiple customers to be managed, please remove or rephrase it to: The proposed solution must provide fine grained role-based access into actions and assets, so users can be granted with investigative actions and not containment actions."	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
268	59	7.6 OEM Responsibilities	1.	All activities relating to solution architecture, design, implementation, configuration, customization, integration, migration, testing, deployment, documentation, training, and Go-Live shall be performed by the respective Solution OEM in coordination with the Bidder	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: 1. All activities relating to solution architecture, design, implementation, configuration, customization, integration, migration, testing, deployment, documentation, training, and Go-Live shall be performed by the respective Solution OEM /OEM authorized partner in coordination with the Bidder. 2. The OEM /OEM authorized partner shall design, implement, and support an enterprise-grade, scalable, resilient, secure, and future-ready solution compatible with the Bank's existing and target IT and Cyber Security architecture across on-premises, cloud, and hybrid environments. 3. The OEM /OEM Authorized partner shall prepare and submit all design documents including HLD, LLD, deployment architecture, integration architecture, configuration guides, SOPs, operational manuals, as-built documentation, and implementation artefacts. 4. The OEM /OEM authorized partner shall provide all native and custom integrations, APIs, connectors, parsers, workflows, playbooks, dashboards, reports, automation, authentication, authorization, RBAC, logging, monitoring, alerting, and interoperability required for successful operation of the solution. 5. The OEM /OEM authorized partner shall perform sizing validation, deployment, migration, configuration, tuning, optimization, health checks, and stabilization to ensure	Please refer addendum for revised clause
269	60	7.16 OEM Services & Deployment (Architecture Assessment)	87	Assessment & performance review 1. Review of respective solutions configurations (Custom parsers, playbooks, controls, rules and process etc.) of the OEM solution 2. System Optimization review and suggestion including remedial actions. 3. Review the bidder's implementation of suggestions of remedial actions. 4. List of Solution for which Assessment is to be conducted, Year 2 Onwards are	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: OEM /OEM authorized partner for Services & Deployment (Architecture Assessment) Assessment & performance review 1. Review of respective solutions configurations (Custom parsers, playbooks, controls, rules and process etc.) of the OEM solution 2. System Optimization review and suggestion including remedial actions. 3. Review the bidder's implementation of suggestions of remedial actions. 4. List of Solution for which Assessment is to be conducted, Year 2 Onwards are	No Change, Please be guided by the RFP
270	60	7.6.1 Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder)		Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder) Requirement Analysis - Activities are to be performed by Respective Solution OEM/OEM Authorized Partner (supported by bidder) 1. The respective Solution OEM, assisted by the bidder, shall conduct a detailed assessment of the Bank's business, functional, technical, operational, security, compliance, and integration requirements and design a scalable, resilient, and futureready solution. The proposed solution shall fully comply with the requirements specified in the RFP and support future business and technology needs of the Bank. 2. As part of the requirement gathering phase, the OEM shall conduct workshops, discovery sessions, interviews, and discussions with the Bank's stakeholders and appointed consultants to understand business requirements, existing infrastructure & solutions, integrations, operational processes, and security requirements. 3. The OEM shall review the Bank's existing IT, security, application, network, cloud, and infrastructure landscape and recommend an optimized target-state architecture leveraging both existing and proposed components wherever feasible.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner Requirement Analysis - Activities are to be performed by Respective Solution OEM/OEM Authorized Partner (supported by bidder) 1. The respective Solution OEM /OEM authorized partner, assisted by the bidder, shall conduct a detailed assessment of the Bank's business, functional, technical, operational, security, compliance, and integration requirements and design a scalable, resilient, and futureready solution. The proposed solution shall fully comply with the requirements specified in the RFP and support future business and technology needs of the Bank. 2. As part of the requirement gathering phase, the OEM/OEM authorized partner shall conduct workshops, discovery sessions, interviews, and discussions with the Bank's stakeholders and appointed consultants to understand business requirements, existing infrastructure & solutions, integrations, operational processes, and security requirements. 3. The OEM /OEM authorized partner shall review the Bank's existing IT, security, application, network, cloud, and infrastructure landscape and recommend an optimized target-state architecture leveraging both existing and proposed components wherever feasible. 4. The OEM /OEM authorized parrtner but not be limited to: a. Requirements elicitation and analysis	No Change, Please be guided by the RFP
271	61	7.6.2 System Design - Activities are to be performed by Respective solution OEM (supported by bidder)	7.6.2	System Design - Activities are to be performed by Respective solution OEM 1. The bidder and respective OEM shall be responsible for the end-to-end design, sizing, customization, configuration, integration, implementation, deployment, maintenance, and support of the proposed solution, including coordination with all associated OEMs, service providers, and stakeholders. 2. All proposed NextGEN SOC solutions shall support seamless interoperability, realtime integration, event sharing, correlation, orchestration, and automated response capabilities to enable unified security operations and minimize manual intervention. 3. The proposed solution shall be configurable and customizable to meet the Bank's functional, technical, operational, reporting, security, and compliance requirements. 4. The bidder and OEM shall design and implement a secure, scalable, resilient, and future-ready architecture based on the approved requirements, data flows, integrations, and operational needs of the Bank. 5. The bidder and OEM shall prepare and submit the following design documents for Bank approval: a. High-Level Design (HLD), including solution	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner System Design - Activities are to be performed by Respective solution OEM/OEM authorized partner (supported by bidder) 1. The bidder and respective OEM /OEM authorized partner shall be responsible for the end-to-end design, sizing, customization, configuration, integration, implementation, deployment, maintenance, and support of the proposed solution, including coordination with all associated OEMs, service providers, and stakeholders. 2. All proposed NextGEN SOC solutions shall support seamless interoperability, realtime integration, event sharing, correlation, orchestration, and automated response capabilities to enable unified security operations and minimize manual intervention. 3. The proposed solution shall be configurable and customizable to meet the Bank's functional, technical, operational, reporting, security, and compliance requirements. 4. The bidder and OEM/OEM authorized partner shall design and implement a secure, scalable, resilient, and future-ready architecture based on the approved requirements, data flows, integrations, and operational needs of the Bank. 5. The bidder and OEM/OEM authorized partner shall prepare and submit the following design documents for Bank approval: a. High-Level Design (HLD), including solution architecture, deployment architecture, integration architecture, and data flow	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
272	61	7.6.3 Development and Installation - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.6.3	1. All installation, configuration, customization, testing, migration, integration, UAT, GoLive, and related implementation activities shall be performed from the Bank's premises. 2. The bidder and respective OEM shall integrate the proposed solution with the Bank's ITSM, SLA Monitoring, monitoring, logging, authentication, and other enterprise platforms, as required. 3. The bidder and OEM shall coordinate with all relevant third parties, OEMs, service providers, and Bank stakeholders to ensure seamless integration, interoperability, and end-to-end functionality of the proposed solution. 4. The bidder shall provide all required integrations, connectors, parsers, APIs, workflows, playbooks, dashboards, reports, alerts, fine-tuning, customizations, enhancements, and remediation activities necessary for successful operation of the solution throughout the contract period without any additional cost to the Bank. 5. The bidder shall adopt and submit an implementation methodology covering solution deployment, customization, testing, managed services, facility management services, knowledge transfer, and hardware/software installation and configuration activities.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Development and Installation - Activities are to be performed by Respective Solution OEM /OEM authorized partner(supported by bidder) 1. All installation, configuration, customization, testing, migration, integration, UAT, GoLive, and related implementation activities shall be performed from the Bank's premises. 2. The bidder and respective OEM/OEM authorized partner shall integrate the proposed solution with the Bank's ITSM, SLA Monitoring, monitoring, logging, authentication, and other enterprise platforms, as required. 3. The bidder and OEM /OEM authorized partner shall coordinate with all relevant third parties, OEMs, service providers, and Bank stakeholders to ensure seamless integration, interoperability, and end-to-end functionality of the proposed solution. 4. The bidder shall provide all required integrations, connectors, parsers, APIs, workflows, playbooks, dashboards, reports, alerts, fine-tuning, customizations, enhancements, and remediation activities necessary for successful operation of the solution throughout the contract period without any additional cost to the Bank. 5. The bidder shall adopt and submit an implementation methodology covering solution deployment, customization,	No Change, Please be guided by the RFP
273	62	7.6.4 Documentation - Activities are to be performed by Respective solution OEM (supported by bidder	7.6.4	The bidder and respective OEM shall prepare, maintain, obtain Bank approval/sign-off, and submit all project, technical, operational, security, and administrative documentation associated with the proposed solution. The indicative list of deliverables shall include, but not be limited to, the following: 1. Detailed Project Plan and Implementation Plan 2. Hardware, Software, Infrastructure, and Sizing Specifications 3. High-Level Design (HLD) and Low-Level Design (LLD) Documents 4. Solution Architecture, Deployment Architecture, and Data Flow Documents 5. Secure Configuration Standards, Baseline Hardening Documents, and Security Configuration Guides 6. System, Database, Integration, Troubleshooting, Diagnostics, and Maintenance Documents 7. Testing, Validation, Acceptance, and Go-Live Documents 8. Change Management, Release Management, Problem Management, and Operational Procedures 9. User Management, Access Management, and Role Administration Guides 10. Release Notes, Impact Assessment Matrix, and Dependency Mapping Documents	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Documentation - Activities are to be performed by Respective solution OEM/OEM authorized partner (supported by bidder The bidder and respective OEM shall prepare, maintain, obtain Bank approval/sign-off, and submit all project, technical, operational, security, and administrative documentation associated with the proposed solution. The indicative list of deliverables shall include, but not be limited to, the following: 1. Detailed Project Plan and Implementation Plan 2. Hardware, Software, Infrastructure, and Sizing Specifications 3. High-Level Design (HLD) and Low-Level Design (LLD) Documents 4. Solution Architecture, Deployment Architecture, and Data Flow Documents 5. Secure Configuration Standards, Baseline Hardening Documents, and Security Configuration Guides 6. System, Database, Integration, Troubleshooting, Diagnostics, and Maintenance Documents 7. Testing, Validation, Acceptance, and Go-Live Documents 8. Change Management, Release Management, Problem Management, and Operational Procedures 9. User Management, Access Management, and Role Administration Guides 10. Release Notes, Impact Assessment Matrix, and Dependency	No Change, Please be guided by the RFP
274	63	7.6.5 Deployment and Go-Live - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.6.5	1. The bidder and respective OEM shall be responsible for deployment of the solution in the production environment, Go-Live planning, implementation, installation, configuration, fine-tuning, migration, stabilization, and hyper care support. 2. The bidder and OEM shall provide onsite support during the hyper care period, monitor solution performance, assist users, conduct training sessions, address issues and defects, implement corrective actions, and recommend operational best practices. 3. The implementation scope shall include deployment planning, migration, testing, validation, issue resolution, user acceptance support, Go-Live execution, and postGo-Live stabilization activities. 4. Prior to Go-Live, the solution shall undergo security validation activities, including VAPT, IS Audit, readiness assessments, identification of security gaps and blind spots, risk remediation, and implementation of recommendations. The Bank or its appointed agency may conduct Continuous Automated Red Teaming, Purple Teaming, security assessments, or other validation exercises as deemed necessary. 5. The bidder and OEM shall conduct performance testing prior to UAT and Go-Live to validate that the	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Deployment and Go-Live - Activities are to be performed by Respective Solution OEM /OEM authorized partner (supported by bidder) 1. The bidder and respective OEM/OEM authorized partner shall be responsible for deployment of the solution in the production environment, Go-Live planning, implementation, installation, configuration, fine-tuning, migration, stabilization, and hyper care support. 2. The bidder and OEM /OEM authorized partner shall provide onsite support during the hyper care period, monitor solution performance, assist users, conduct training sessions, address issues and defects, implement corrective actions, and recommend operational best practices. 3. The implementation scope shall include deployment planning, migration, testing, validation, issue resolution, user acceptance support, Go-Live execution, and postGo-Live stabilization activities. 4. Prior to Go-Live, the solution shall undergo security validation activities, including VAPT, IS Audit, readiness assessments, identification of security gaps and blind spots, risk remediation, and implementation of recommendations. The Bank or its appointed agency may conduct Continuous Automated Red Teaming, Purple Teaming, security assessments,	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
275	64	7.6.6 Testing- Activities are to be performed by Respective solution OEM (supported by bidder)	7.6.6	1. The Bank shall conduct User Acceptance Testing (UAT) to validate that the proposed solution and all associated components, integrations, workflows, reports, dashboards, and functionalities comply with the requirements specified in the RFP, approved FRSM/SRS, and other project documents. 2. The bidder and respective OEM shall confirm completion of all implementations, configuration, customization, integration, migration, and testing activities prior to commencement of UAT and certify that the solution is ready for user validation. 3. The bidder shall provision and maintain dedicated Development, Testing, UAT, and Pre-Production environments throughout the contract period. All software, licenses, and other resources required for such environments shall be included within the bidder's scope without any additional cost to the Bank. 4. Any defects, deviations, vulnerabilities, observations, or non-compliances identified during UAT, security assessments, audits, reviews, or validation exercises shall be rectified by the bidder within the timelines prescribed by the Bank and at no additional cost. 5. The bidder shall maintain appropriate version control, configuration management, change	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Testing- Activities are to be performed by Respective solution OEM/OEM authorized partner (supported by bidder) 1. The Bank shall conduct User Acceptance Testing (UAT) to validate that the proposed solution and all associated components, integrations, workflows, reports, dashboards, and functionalities comply with the requirements specified in the RFP, approved FRSM/SRS, and other project documents. 2. The bidder and respective OEM /OEM authorized partner shall confirm completion of all implementations, configuration, customization, integration, migration, and testing activities prior to commencement of UAT and certify that the solution is ready for user validation. 3. The bidder shall provision and maintain dedicated Development, Testing, UAT, and Pre-Production environments throughout the contract period. All software, licenses, and other resources required for such environments shall be included within the bidder's scope without any additional cost to the Bank. 4. Any defects, deviations, vulnerabilities, observations, or non-compliances identified during UAT, security assessments, audits, reviews, or validation exercises shall be rectified by the bidder within the timelines prescribed by the Bank and at no additional cost.	No Change, Please be guided by the RFP
276	65	7.6.6.1 Quality Assurance	7.6.6.1	1. Testing Requirements a. The respective OEM shall be responsible for planning, executing, documenting, and successfully completing all testing activities required to validate the functionality, performance, stability, reliability, security, interoperability, and operational readiness of the proposed solution. The bidder shall prepare detailed test plans, test cases, test data, automation scripts (where applicable), entry and exit criteria, test reports, defect logs, root cause analysis reports, workarounds, and remediation plans, and shall obtain the Bank's approval wherever required. 2. Test Preparation The respective OEM shall: a. Prepare the overall testing strategy and methodology for Unit Testing (UT), UAT, Performance Testing, Security Testing, and other applicable tests. b. Establish and maintain the required test environments, infrastructure, software, applications, and test data. c. Prepare, validate, and execute test cases, scripts, and automation frameworks, wherever applicable. d. Define test entry and exit criteria, acceptance criteria, and success parameters. 3. Test Execution The respective OEM shall: a. Execute all approved test cases and scripts. b. Record, track, report, and resolve defects,	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: 1. Testing Requirements a. The respective OEM/OEM authorized partner shall be responsible for planning, executing, documenting, and successfully completing all testing activities required to validate the functionality, performance, stability, reliability, security, interoperability, and operational readiness of the proposed solution. The bidder shall prepare detailed test plans, test cases, test data, automation scripts (where applicable), entry and exit criteria, test reports, defect logs, root cause analysis reports, workarounds, and remediation plans, and shall obtain the Bank's approval wherever required. 2. Test Preparation The respective OEM /OEM authorized partner shall: a. Prepare the overall testing strategy and methodology for Unit Testing (UT), UAT, Performance Testing, Security Testing, and other applicable tests. b. Establish and maintain the required test environments, infrastructure, software, applications, and test data. c. Prepare, validate, and execute test cases, scripts, and automation frameworks, wherever applicable. d. Define test entry and exit criteria, acceptance criteria, and success parameters. 3. Test Execution The respective OEM /OEM authorized partner	No Change, Please be guided by the RFP
277	66	7.6.7 Training- Activities are to be performed by Respective solution OEM (supported by bidder)	7.6.7	7.6.7 Training- Activities are to be performed by Respective solution OEM (supported by bidder) The bidder and respective OEMs shall provide comprehensive product training, knowledge transfer, and certification programs for the Bank's IT and Information Security personnel at no additional cost. All technical and product-specific training shall be delivered by OEM. Upon successful completion of the training programs, the respective OEM shall issue participation and/or certification certificates to the attendees. The bidder shall submit a detailed Training and Certification Plan covering training objectives, curriculum, skill levels, training schedules, participant eligibility, certification pathways, and assessment criteria. The training program shall cover product functionalities, administration, troubleshooting, maintenance, security best practices, automation, advanced threat scenarios, security monitoring and analysis, incident response and investigation, threat detection and hunting, intelligence analysis, new features, upgrades, operational workflows, and relevant industry trends. Bidder along with the OEM should provision the training & certification of the bank's relevant officials from the relevant Cloud service provider where the	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Training- Activities are to be performed by Respective solution OEM **/OEM Authorized partner (supported by bidder)** The bidder and respective OEMs /OEM authorized partner shall provide comprehensive product training, knowledge transfer, and certification programs for the Bank's IT and Information Security personnel at no additional cost. All technical and product-specific training shall be delivered by OEM/OEM Authorized partner. Upon successful completion of the training programs, the respective OEM /OEM Authorized partner shall issue participation and/or certification certificates to the attendees. The bidder shall submit a detailed Training and Certification Plan covering training objectives, curriculum, skill levels, training schedules, participant eligibility, certification pathways, and assessment criteria. The training program shall cover product functionalities, administration, troubleshooting, maintenance, security best practices, automation, advanced threat scenarios, security monitoring and analysis, incident response and investigation, threat detection and hunting, intelligence analysis, new features, upgrades, operational workflows, and relevant industry trends. Bidder along with the OEM/OEM authorized partner should provision the training & certification of the bank's relevant officials from the relevant	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
278	67	7.6.8 Security requirements - Activities are to be performed by Respective solution OEM (supported by bidder)	7.6.8	1. The bidder and respective OEMs shall comply with the Bank's IT, Information Security, Cyber Security, Data Protection, Privacy, Business Continuity, and related policies, standards, procedures, and guidelines, as shared by the Bank from time to time. The bidder shall be responsible for ensuring the confidentiality, integrity, availability, security, and privacy of the Bank's information assets, systems, applications, and data throughout the contract period. 2. The bidder shall implement and maintain appropriate administrative, technical, physical, and operational controls for protection of data, applications, systems, infrastructure, and associated assets under its custody or management. 3. The bidder shall comply with the Bank's requirements relating to access management, privileged access management, password policies, user administration, data protection, encryption, monitoring, incident management, and security governance. 4. The bidder shall ensure encryption and protection of data at rest, data in transit, and data in use, wherever applicable, using industry-standard security controls and cryptographic mechanisms. All tools, technologies, and controls required to achieve the same shall form part of the proposed solution.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Security requirements - Activities are to be performed by Respective solution OEM/OEM authorized partner (supported by bidder) 1. The bidder and respective OEMs/OEM authorized partner shall comply with the Bank's IT, Information Security, Cyber Security, Data Protection, Privacy, Business Continuity, and related policies, standards, procedures, and guidelines, as shared by the Bank from time to time. The bidder shall be responsible for ensuring the confidentiality, integrity, availability, security, and privacy of the Bank's information assets, systems, applications, and data throughout the contract period. 2. The bidder shall implement and maintain appropriate administrative, technical, physical, and operational controls for protection of data, applications, systems, infrastructure, and associated assets under its custody or management. 3. The bidder shall comply with the Bank's requirements relating to access management, privileged access management, password policies, user administration, data protection, encryption, monitoring, incident management, and security governance. 4. The bidder shall ensure encryption and protection of data at rest, data in transit, and data in use, wherever applicable, using	No Change, Please be guided by the RFP
279	70	7.7 On-cloud proposed solution OEM Responsibilities	7.6.9	1. The security telemetry received by the OEM Cloud platform will be routed to the dedicated tenant/workspace provisioned for the Bank.	What is the requirement here, is it required to maintain a copy of all cloud data to a local instance /data lake, please clarify, who need to provision this, does bank has this instance available, if not required please remove this ask.	The security telemetry received and processed by the OEM Cloud/SaaS platform shall be logically segregated and maintained within a dedicated tenant/workspace provisioned for the Bank. The dedicated tenant/workspace shall ensure segregation of the Bank's security data, configurations, policies, analytics, alerts, incidents and other Bank-related information from those of other customers.
280	71	7.10 Data Privacy	7.1 0	Executive Governance and Project Oversight 1. The bidder and each respective OEM shall nominate a senior executive as the Project Sponsor/Project Director responsible for executive governance, stakeholder management, escalation management, strategic oversight, and overall project success. 2. The Project Sponsor, Project Director, and designated senior representatives of the bidder and OEMs shall participate in governance meetings, executive reviews, strategy workshops, and escalation meetings as required by the Bank. An, On quarterly/or as per the frequency defined by bank, executive governance meetings shall be conducted throughout the contract period to review project progress, service delivery, operational performance, security posture, compliance, risks, technology enhancements, and continuous improvement opportunities. 3. The bidder and OEMs shall deploy and maintain adequately skilled, certified, experienced, and qualified resources, together with appropriate backup resources, succession planning, and skill development mechanisms, to ensure uninterrupted 24x7x365 service delivery throughout the contract period.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Executive Governance and Project Oversight 1. The bidder and each respective OEM/OEM authorized partner shall nominate a senior executive as the Project Sponsor/Project Director responsible for executive governance, stakeholder management, escalation management, strategic oversight, and overall project success. 2. The Project Sponsor, Project Director, and designated senior representatives of the bidder and OEMs /OEM authorized partner shall participate in governance meetings, executive reviews, strategy workshops, and escalation meetings as required by the Bank. An, On quarterly/or as per the frequency defined by bank, executive governance meetings shall be conducted throughout the contract period to review project progress, service delivery, operational performance, security posture, compliance, risks, technology enhancements, and continuous improvement opportunities. 3. The bidder and OEMs /OEM Authorized partner shall deploy and maintain adequately skilled, certified, experienced, and qualified resources, together with appropriate backup resources, succession planning, and skill development mechanisms, to ensure uninterrupted 24x7x365 service delivery throughout the contract period. 4. The bidder shall establish and maintain a Bank-approved	Please refer addendum for revised clause
281	72	7.12 Resource Requirement	7.6.12	7.12.1Implementation Phase • Prior to commencement of implementation, the bidder and respective OEMs shall submit a detailed Resource Deployment Plan for Bank approval identifying proposed onsite and offsite resources, roles, responsibilities, certifications, experience, deployment schedules, and solution-wise allocation. • The bidder shall deploy a dedicated onsite Project Manager throughout the implementation phase and nominate appropriate bidder and OEM resources for each solution, workstream, milestone, and project activity. • Any replacement, redeployment, or modification of approved implementation resources shall require prior written approval from the Bank.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Implementation Phase • Prior to commencement of implementation, the bidder and respective OEMs /OEM authorized partner shall submit a detailed Resource Deployment Plan for Bank approval identifying proposed onsite and offsite resources, roles, responsibilities, certifications, experience, deployment schedules, and solution-wise allocation. • The bidder shall deploy a dedicated onsite Project Manager throughout the implementation phase and nominate appropriate bidder and OEM /OEM authorized partner resources for each solution, workstream, milestone, and project activity. • Any replacement, redeployment, or modification of approved implementation resources shall require prior written approval from the Bank.	No Change, Please be guided by the RFP
282	72	7.12.2Operations and Maintenance (O&M) Phase		7.12.2Operations and Maintenance (O&M) Phase • The bidder shall deploy the minimum onsite L1, L2, Project Manager/L3 – Operations, and other resources specified in the RFP and ensure uninterrupted 24x7x365 support through an appropriate shift-based deployment model. • The respective OEMs shall provide subject matter experts from the date of installation throughout the contract period to support operations, troubleshooting, optimization, upgrades, audits, vulnerability remediation, and major incidents. • The bidder shall ensure adequate SME support for timely resolution of incidents, service requests, problems, vulnerabilities, and operational issues.	O & M shall be bidders responsibility pleaase remove OEM from this to maintain right availability and cost Operations and Maintenance (O&M) Phase • The bidder shall deploy the minimum onsite L1, L2, Project Manager/L3 – Operations, and other resources specified in the RFP and ensure uninterrupted 24x7x365 support through an appropriate shift-based deployment model. • The respective bidder shall provide subject matter experts from the date of installation throughout the contract period to support operations, troubleshooting, optimization, upgrades, audits, vulnerability remediation, and major incidents. • The bidder shall ensure adequate SME support for timely resolution of incidents, service requests, problems, vulnerabilities, and operational issues.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
283	73	7.12.3Resource Management and Governance	7.12	OEM Implementation Resources Onsite (Full Time) OEM shall submit a detailed resource deployment plan before commencement of requirement gathering. Any replacement or modification shall require prior Bank approval.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: OEM /OEM authorized partner Implementation Resources Onsite (Full Time) OEM/OEM authorized partner shall submit a detailed resource deployment plan before commencement of requirement gathering. Any replacement or modification shall require prior Bank approval.	No Change, Please be guided by the RFP
284		7.17 System recovery	1	. In case of disaster, it is the responsibility of the Respective solution OEM along with the bidder to ensure that services remain unaffected and same is up and running from secondary site (DR)	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: . In case of disaster, it is the responsibility of the Respective solution OEM/OEM Authorized partner along with the bidder to ensure that services remain unaffected and same is up and running from secondary site (DR)	No Change, Please be guided by the RFP
285		7.19 Other In-Scope Services	7.19	7.19.1Other Scope Activity 1. The Respective solution OEM along with the bidder is expected to ensure that all functionalities as mentioned in Appendix 1A: Functional Specification are made available to PSB. 2. The Respective solution OEM along with the bidder is expected to ensure that for the purpose of this RFP, statutory and regulatory changes shall mean any change prescribed by the statutory and regulatory bodies governing/ affecting the banking industry in India viz. Reserve Bank of India, Ministry of Finance, CCIL, NPCI, IBA, SEBI, or any such bodies constituted by the RBI mandating change/s to an existing functionality of the Solution shall be provided to the Bank at no additional cost for the entire contract period. However, any Statutory and Regulatory changes post Go-Live of the respective applications (which are not a part of the existing functionalities) will be on CR basis based on the rates provided in the Bill of Material. 3. The Respective Solution OEM along with the bidder is expected to carry out a requirement study for the functionalities and services required by PSB, to gain understanding of the business requirements. 4. Respective solution OEM along with the bidder	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: 1Other Scope Activity 1. The Respective solution OEM/OEM Authorized partner along with the bidder is expected to ensure that all functionalities as mentioned in Appendix 1A: Functional Specification are made available to PSB. 2. The Respective solution OEM/OEM Authorized partner along with the bidder is expected to ensure that for the purpose of this RFP, statutory and regulatory changes shall mean any change prescribed by the statutory and regulatory bodies governing/ affecting the banking industry in India viz. Reserve Bank of India, Ministry of Finance, CCIL, NPCI, IBA, SEBI, or any such bodies constituted by the RBI mandating change/s to an existing functionality of the Solution shall be provided to the Bank at no additional cost for the entire contract period. However, any Statutory and Regulatory changes post Go-Live of the respective applications (which are not a part of the existing functionalities) will be on CR basis based on the rates provided in the Bill of Material. 3. The Respective Solution OEM/OEM Authorized partner along with the bidder is expected to carry out a requirement study for the functionalities and services required by PSB, to gain understanding of the business requirements. 4. Respective solution OEM /OEM Authorized partner along	Please refer addendum for revised clause
286		7.19.4DR Setup - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.19.4	DR Setup - Activities are to be performed by Respective Solution OEM (supported by bidder) 1. Respective solution OEM along with the bidder has to ensure that DR setup is ready on the date of Go Live of respective Applications 2. Respective solution OEM along with the bidder should make necessary setup to enable the DR within the agreed timelines. 3. Respective solution OEM along with the bidder should carry out the deployment of the application in DC and DR, UAT as applicable. 4. To ensure proper rollback, Respective solution OEM along with the bidder has to ensure that the old setup at all the locations is as–IS as per the agreed timelines during migration strategy formulation	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner DR Setup - Activities are to be performed by Respective Solution OEM /OEM authorized partner (supported by bidder) 1. Respective solution OEM /OEM Authorized partneralong with the bidder has to ensure that DR setup is ready on the date of Go Live of respective Applications 2. Respective solution OEM/OEM Authorized partner along with the bidder should make necessary setup to enable the DR within the agreed timelines. 3. Respective solution OEM/OEM Authrized partner along with the bidder should carry out the deployment of the application in DC and DR, UAT as applicable. 4. To ensure proper rollback, Respective solution OEM/OEM Authrized partner along with the bidder has to ensure that the old setup at all the locations is as–IS as per the agreed timelines during migration strategy formulation	No Change, Please be guided by the RFP
287		13 SERVICE LEVELS & PENALTIES	2	2. The bidder and the OEM shall be jointly responsible for the maintenance, configuration, performance, and fault-free operation of the entire supplied infrastructure, including hardware, software, operating systems, databases, and related components, during the warranty, AMC, ATS, and FMS periods, as applicable	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: The bidder and the OEM /OEM authorized partner shall be jointly responsible for the maintenance, configuration, performance, and fault-free operation of the entire supplied infrastructure, including hardware, software, operating systems, databases, and related components, during the warranty, AMC, ATS, and FMS periods, as applicable	No Change, Please be guided by the RFP
288	159	14.1 Assignment & Subcontracting	1	The selected bidder shall not subcontract/JV/Consortium or permit anyone to perform any of the work, service or other performance required under the contract (excluding Proposed OEM personnels). All bidder's personnel proposed for the bank shall be on bidder's Payroll. Bank will seek relevant documentation from the bidder to validate the same.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: The selected bidder shall not subcontract/JV/Consortium or permit anyone to perform any of the work, service or other performance required under the contract (excluding Proposed OEM /OEM Autorized partner personnels). All bidder's personnel proposed for the bank shall be on bidder's Payroll. Bank will seek relevant documentation from the bidder to validate the same.	No Change, Please be guided by the RFP
289	101	10 EVALUATION CRITERIA	10.2 Eligibility Evaluation Criteria Clause no 4	The bidder should have a minimum average turnover of INR 500 crore per annum in India during the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth. Note – In case of MSMEs only, the turnover may be relaxed subject to meeting the quality and technical specifications	Please modify the clause as requested below:- The bidder should have a minimum average turnover of INR 300 crore per annum in India during the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth. Note – In case of MSMEs only, the turnover may be relaxed subject to meeting the quality and technical specifications	No Change, Please be guided by the RFP
290	101	10 EVALUATION CRITERIA	10.2 Eligibility Evaluation Criteria Clause no 6	Bidder must have at least enrolled manpower (on bidder's payroll) of 100 experienced employees skilled in areas of Cyber security.	Bidder must have at least enrolled manpower (on bidder's payroll) of 30 experienced employees skilled in areas of Cyber security.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
291	101-102	10 EVALUATION CRITERIA	10.2 Eligibility Evaluation Criteria Clause no 8	Bidder should have supplied, installed and maintained (or under maintenance) any three (3) of the below solutions in any one PSU/PSE/ Government Organizations / BFSI/Telecom provider in India a. SOAR b. UEBA c. Extended Detection & response (XDR)/ Endpoint Detection & response (EDR) d. Network Detection & response (NDR)/Network Behaviour Anomaly Detection (NBAD) e. Threat Intelligence Platform f. Vulnerability Assessment/Vulnerability management g. Identity Threat Detection & response h. Decoy/Honeypot/Deception i. Application security testing tool (DAST or SAST) j. Cloud Security Posture Management (CSPM) k. Cloud-Native Application Protection Platform (CNAPP) l. Cloud Workload Protection Platform (CWPP) m. Continuous Threat Exposure Management (CTEM)	Please modify the clause as requested below:- Bidder should have supplied, installed and maintained (or under maintenance) any three (3) of the below solutions in any one PSU/PSE/ Government Organizations / BFSI/Telecom provider in India a. SOAR b. UEBA c. Extended Detection & response (XDR)/ Endpoint Detection & response (EDR) d. Network Detection & response (NDR)/Network Behaviour Anomaly Detection (NBAD) e. Threat Intelligence Platform f. Vulnerability Assessment/Vulnerability management g. Identity Threat Detection & response h. Decoy/Honeypot/Deception i. Application security testing tool (DAST or SAST) j. Cloud Security Posture Management (CSPM) k. Cloud-Native Application Protection Platform (CNAPP) l. Cloud Workload Protection Platform (CWPP) m. Continuous Threat Exposure Management (CTEM) n. SIEM o. WAF p. Next Generation Firewall q.Privileged Access Management (PAM) r. Data Loss Protection (DLP) solution	Please refer addendum for the revised clause
292	PBQ-02	Annexure 21, 16.21.1 and 16.21.2 (p.257-258)	16.21.2 states 'XDR solution for 12,000 users scalable to 14,000'. 16.21.1 separately lists 2,500 servers and 300 databases, alongside 12,000 branch desktops.	The Bank is requested to confirm whether the XDR quantity of 12,000 covers desktops only, or whether the 2,500 servers listed at 16.21.1 are also to be covered within that count. If servers are in scope, the Bank is requested to confirm the split between desktop and server quantities so that both can be quoted correctly.	Section 7.3.4 states XDR coverage 'across endpoints and servers'. If servers are deemed in scope after award, the bid is 2,500 licences short at a different unit price, with no mechanism to re-price. This is the largest commercial exposure on the XDR line.	Bank has given the requirement of 12,000 desktops scalable to 16000
293	PBQ-03	Section 3, clause 6 and clause 11	All Bank data shall reside within India. No Bank data shall be transmitted, replicated, processed, accessed, stored or exchanged outside India without prior written approval from the Bank and applicable regulatory permissions.	The Bank is requested to confirm that OEM technical support and engineering access to Bank data, performed under a documented, logged and auditable process and subject to the Bank's prior written approval as already contemplated in the clause, satisfies this requirement — with all storage and processing remaining within the India region.	Storage and processing within India is achievable. The clause additionally restricts ACCESS, and global OEM support operates on a follow-the-sun basis. Without this clarification the clause cannot be answered 'Complied' truthfully, and Section 15.1 forbids a conditional answer.	Storage and processing of Bank data shall be within India as sought in the RFP. Any access to Bank data from outside India, including access by OEM/Bidder support or engineering personnel, shall require prior written approval of the Bank. Such access, if approved, shall be through secure, controlled and auditable mechanisms, on a least-privilege basis, with appropriate logging and monitoring on case to case basis only
294	PBQ-04	Section 7.2.4, Cloud/SaaS table (p.37); Annexure 21, 16.21.3 (p.261)	All Bank-owned data including logs, configurations, policies, rules, reports and metadata shall be backed up / transferred to the Bank's backup infrastructure at DC and DR, with monthly full backups retained in Long-Term Storage for the entire contract duration.	The Bank is requested to confirm whether the endpoint telemetry to be transferred to Bank infrastructure may be scoped to a defined security-relevant subset agreed during implementation and documented in the SOP, rather than the complete raw telemetry stream. Bidders would appreciate an indicative Bank position so that Long-Term Storage can be sized correctly at bid stage.	Unfiltered endpoint telemetry for the proposed estate is of the order of hundreds of GB per day compressed, which over a five-year retention obligation becomes a very large and expensive Bank-side storage requirement. Scoping this at bid stage protects both the Bank's cost and the Bidder's sizing.	All Bank-owned data falling within the stated scope shall be backed up/transferred in accordance with the RFP requirements.
295	PBQ-05	Annexure 21, 16.21.2 (p.258-259)	'Each node/environment must be individually provisioned for full peak load' and 'all inline components must operate in high availability mode with automatic failover within seconds'.	For Cloud/SaaS delivered solutions, the Bank is requested to confirm that these requirements apply to the Bank-side components deployed at DC and DR, and that the SaaS platform's availability and capacity are governed by the service levels, RTO and RPO specified in Section 13.	Node-level provisioning commitments cannot be made against multi-tenant SaaS infrastructure. Without this clarification the OEM would be signing an obligation it does not control.	For Cloud/SaaS The bidder/OEM is responsible for sizing and provisioning the required cloud resources, including compute, storage, databases, containers, networking, load balancers and associated services, and for ensuring capacity, HA, fault tolerance, DR, scalability and service continuity in accordance with the RFP. however, the bidder/OEM remains fully accountable for the resulting service performance, availability, resilience and SLA compliance. Capacity shortfalls affecting the contracted service shall be addressed by the bidder at no additional cost to the Bank, as specified in the RFP.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
296	PBQ-06	Section 3, clause 12	Bank data shall not be used for model training, retraining, analytics, or shared with third parties, whatsoever, except as explicitly authorised by the Bank in writing.	The Bank is requested to confirm whether this restriction is intended to preclude the use of anonymised and aggregated threat indicators for the purpose of improving threat detection efficacy for the Bank's own environment, or whether it is intended to apply without exception.	Determines whether any AI-assisted or threat-intelligence-derived capability can be offered at all, and shapes the OEM's Data Processing Addendum position. Must be settled before the Annexure 18 declaration is signed.	Bank data shall not be used for model training, model retraining, analytics or shared with third parties except where explicitly authorised by the Bank in writing. Any proposed use of Bank-derived data, telemetry, prompts, metadata, indicators or other information for improving models, services or analytics shall require the Bank's prior written approval
297	PBQ-07	Eligibility criteria #24 and #25 (p.210-211); Section 15.1 (p.169)	Minimum 85% functional compliance per solution against Appendix 1A, with exceptions, disclaimers, limitations and conditional compliance not taken on record.	The Bank is requested to confirm whether a response of 'Complied through an additional licensed module included in the commercial offer' is treated as Complied for functional compliance scoring purposes, given that the module concerned is being quoted and supplied as part of the proposal.	Several capabilities are delivered through licensed add-ons that are being priced in the BOQ. Confirming this treatment prevents a technically compliant, fully priced solution being marked down for describing how a capability is licensed.	The bidder shall ensure that all functionalities and requirements specified in the FRS and Scope of Work are fully met without any additional cost to the Bank. Accordingly, the bidder shall factor in all associated costs, including but not limited to software licenses, infrastructure, hardware, implementation, integration, configuration, upgrades, support, and any other components necessary for fulfilling the specified requirements, in its commercial bid.
298	PBQ-08	Eligibility criteria #24 and #25 (p.210-211)	Compliance confirmation and 85% functional compliance are required for each of 14 listed solutions and 9 listed services.	The Bank is requested to confirm that bids comprising multiple OEMs across the listed solutions are permitted, with each OEM providing the Annexure 18 declaration and Appendix 1A compliance for the solutions it supplies.	No single OEM supplies all 14 solutions and 9 services. Confirming the multi-OEM position protects the bid structure.	The compliance of 85% should be met by each of the OEM for their respective Solution & Services as per the eligibility criteria defined.
299	37	7.2.4.3 Storage and other Requirement	Primary Log Storage & Retention	Parsed, normalized, enriched, indexed and correlated logs, together with associated metadata and contextual information,shall be retained for a minimum period of 60 months (5 years)	Please clarify for how much period the past log should be searchable under the platform, example one year of searchable next four years archival	Please refer addendum for the revised clause
300			Primary Log Storage & Retention	together with associated metadata and contextual information,		Delete
301			Primary Log Storage & Retention	shall be retained for a minimum period of 60 months (5 years)		Delete
302	39	7.3.1.1 Modules, Architecture & Deployment:		The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Please provide the details of current MFA solution	The proposed solution shall, by default, provide native Two-Factor Authentication (2FA)/Multi-Factor Authentication (MFA) capability as an integral security feature. The solution shall also be capable of integrating with the Bank's existing MFA solution, if the Bank elects to use the Bank's existing MFA solution for authentication. Where such integration is required by the Bank, the Bank may provide necessary technical details or reasonable support for integration. The Bidder and OEM shall be responsible for ensuring compatibility, configuration and implementation of the required integration as part of their scope.
303				capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.		Delete
304	42	7.3.1.3 Key Deliverables:	7	The solution shall provide a consolidated Enterprise SOC dashboard providing an integrated view of SIEM, XDR, SOAR, UEBA, threat intelligence, and other relevant cybersecurity components.	please clarify do bidder need to make a single dashboard for all the components	No Change, Please be guided by the RFP, Clause 7.3.1.3 (Key Deliverables), Point 7, which requires a single consolidated Enterprise SOC dashboard providing an integrated view across SIEM, XDR, SOAR, UEBA, threat intelligence and other relevant components - not separate, siloed dashboards per tool
305				integrated view of SIEM, XDR, SOAR, UEBA, threat intelligence, and other relevant		Delete
306				cybersecurity components.		Delete
307	65	7.6.6.1 Quality Assurance	2 Test Environment	Prepare the overall testing strategy and methodology for Unit Testing (UT), UAT, Performance Testing, Security Testing, and other applicable tests.	Please clarify, do we need to set up a separate test environment? If yes what are the please provide the configuration details	the Bidder shall design, size and provision the test environment per these clauses, in consultation with the respective OEMs, as part of Clause 7.6.6.1's testing obligations.
308				UAT, Performance Testing, Security Testing, and other applicable tests.		Delete
309		SIEM Compliances	Supported Data sources	The solution should have the capability to identify / remember frequently used queries	please clarify what kind of Queries PSB wish to run	No Change, Please be guided by the RFP
310			page 40			Delete
311			16.21.2 Volumetrics-Solution-wise Requirements: 6 NDR		Requesting bank to modify clause to "Throughput requirement of 10 Gbps. Critical components must support High Availability (HA) / N+1 redundancy or clustered fault tolerance. In the event of a node degradation or failure, the platform must preserve continuous visibility and data integrity without dropping network traffic. Each node/environment must be individually provisioned for full peak load." for wider participation	Please refer addendum for the revised clause
312			7.2.1 Solutions – Master Deployment Matrix		Requesting bank to modify the caluse to "Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, N+1 redundancy at DC and DR. Management Console: Deployed at both DC and DR " for wider participation	Please refer addendum for the revised clause
313			7.2.4.1 Deployment Pattern		Requesting Bank to modify to "The NDR solution shall be deployed On-Premises across the Bank's DC and DR sites with the required Telemetry collection and storage tiers in High Availability (HA) / Active-Active scale-out clustering or N+1 redundancy at the respective sites." for wider participation.	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
314			Appendix 1A: NDR: Required Functionalities:3	Proposed solution should be a scale out dedicated purpose built solution that must provide full Detection, Network Visibility, Investigation & Forensic capability / Back in Time investigation, through high speed lossless packet capture & analysis functions for a network traffic capture for 10 Gbps.	Request bank to modify clause to " Proposed solution should be a scale out dedicated purpose built solution that must provide end-to-end network visibility, behavioral anomaly detection, advanced threat investigation, and forensic capability/ back-in-time investigation, through unsampled or deep-packet-derived lossless flow telemetry (NetFlow, IPFIX) and metadata extraction capable of monitoring 10 Gbps." for wider participation.	Please refer addendum for revised clause.
315			Appendix 1A: NDR: Required Functionalities:4	The solution should support Network Behaviour Anomaly detection using full Packet data including L3 / L4 and L7 headers. System should have continuous learning of the traffic baseline and detecting any anomaly for the learned baseline with respect to traffic volume, traffic directionality, protocol usage and unseen application or any specific host / endpoint / user behaving differently	Request to change to "The solution should support Network Behaviour Anomaly detection using deep packet inspection (DPI) and enriched telemetry, including L3/L4 and L7 header/application/cryptographic metadata. System should have continuous learning of the traffic baseline and detecting any anomaly for the learned baseline with respect to traffic volume, traffic directionality, protocol usage and unseen application or any specific host / endpoint / user behaving differently." for wider participation.	Please refer addendum for the revised clause
316			Appendix 1A: NDR: Required Functionalities:5	Solution should support below protocols monitoring and also Solution should provide detailed packet decode and analysis for the same.	Request to change to " Solution should support below application/protocol identification, metadata extraction, and flow-based behavioral analysis via deep packet inspection. " for wider participation.	Please refer addendum for the revised clause
317			Appendix 1A: NDR: Required Functionalities:13		Requesting to change this point to " The proposed solution shall feature a centralized, highly available management and analytics console delivering customizable security dashboards with dynamic role-based access controls. The administration interface must support high availability / disaster recovery architecture ensuring seamless access and data resilience across the Bank's Primary and Disaster Recovery sites. " for wider participation for On-prem solution vendors. Requesting bank to clarify if solution needs to be hosted on Cloud. As per Sec 7.2.1 Solutions needs to be on-premise hardware/virtual.	Please refer addendum for the revised clause
318	23	SIEM / Functional Specification	23	Where a native parser or connector is unavailable, the proposed solution shall provide supported mechanisms, SDKs, APIs, templates, or configuration interfaces to develop and maintain custom integrations	For a recuced overall TCO and ensure the timely availability without any delay, please rephrase it to: OEM /OEM authorized partner to provide parsers for data ingestion for all the current data sources and their respective upgrades (in maximum 15 business days from data of intimation of the same) during the contract period. If any new data source is added during the contract period, the OEM will provide parsers for data ingestion in maximum 15 business days from data of intimation of the same, without dependency of the bidder.	No Change, Please be guided by the RFP
319	28	SIEM / Incident Response	131	The proposed cloud-delivered solution shall provide secure multi-tenant architecture with appropriate logical tenant isolation, encryption in transit and at rest, secure authentication, MFA, granular RBAC, audit logging and protection of Bank security data in accordance with the approved service architecture, security controls and SLA.	Why there is a need for multi-tennacy, this is specially required in a service provider environment needing multiple customers to be managed, please remove or rephrase it to: The proposed solution must provide fine grained role-based access into actions and assets, so users can be granted with investigative actions and not containment actions."	Please refer addendum for the revised clause
320	59	7.6 OEM Responsibilities	1.	All activities relating to solution architecture, design, implementation, configuration, customization, integration, migration, testing, deployment, documentation, training, and Go-Live shall be performed by the respective Solution OEM in coordination with the Bidder	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: 1. All activities relating to solution architecture, design, implementation, configuration, customization, integration, migration, testing, deployment, documentation, training, and Go-Live shall be performed by the respective Solution OEM /OEM authorized partner in coordination with the Bidder. 2. The OEM /OEM authorized partner shall design, implement, and support an enterprise-grade, scalable, resilient, secure, and future-ready solution compatible with the Bank's existing and target IT and Cyber Security architecture across on-premises, cloud, and hybrid environments. 3. The OEM /OEM Authorized partner shall prepare and submit all design documents including HLD, LLD, deployment architecture, integration architecture, configuration guides, SOPs, operational manuals, as-built documentation, and implementation artefacts. 4. The OEM /OEM authorized partner shall provide all native and custom integrations, APIs, connectors, parsers, workflows, playbooks, dashboards, reports, automation, authentication, authorization, RBAC, logging, monitoring, alerting, and interoperability required for successful operation of the solution. 5. The OEM /OEM authorized partner shall perform sizing validation, deployment, migration, configuration, tuning, optimization, health checks, and stabilization to ensure	Please refer addendum for revised clause
321	60	7.16 OEM Services & Deployment (Architecture Assessment)	87	Assessment & performance review 1. Review of respective solutions configurations (Custom parsers, playbooks, controls, rules and process etc.) of the OEM solution 2. System Optimization review and suggestion including remedial actions. 3. Review the bidder's implementation of suggestions of remedial actions. 4. List of Solution for which Assessment is to be conducted, Year 2 Onwards are	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: OEM /OEM authorized partner for Services & Deployment (Architecture Assessment) Assessment & performance review 1. Review of respective solutions configurations (Custom parsers, playbooks, controls, rules and process etc.) of the OEM solution 2. System Optimization review and suggestion including remedial actions. 3. Review the bidder's implementation of suggestions of remedial actions. 4. List of Solution for which Assessment is to be conducted, Year 2 Onwards are	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
322	60	7.6.1 Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder)		Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder) Requirement Analysis - Activities are to be performed by Respective Solution OEM/OEM Authorized Partner (supported by bidder) 1. The respective Solution OEM, assisted by the bidder, shall conduct a detailed assessment of the Bank's business, functional, technical, operational, security, compliance, and integration requirements and design a scalable, resilient, and futureready solution. The proposed solution shall fully comply with the requirements specified in the RFP and support future business and technology needs of the Bank. 2. As part of the requirement gathering phase, the OEM shall conduct workshops, discovery sessions, interviews, and discussions with the Bank's stakeholders and appointed consultants to understand business requirements, existing infrastructure & solutions, integrations, operational processes, and security requirements. 3. The OEM shall review the Bank's existing IT, security, application, network, cloud, and infrastructure landscape and recommend an optimized target-state architecture leveraging both existing and proposed components wherever feasible.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner Requirement Analysis - Activities are to be performed by Respective Solution OEM/OEM Authorized Partner (supported by bidder) 1. The respective Solution OEM /OEM authorized partner, assisted by the bidder, shall conduct a detailed assessment of the Bank's business, functional, technical, operational, security, compliance, and integration requirements and design a scalable, resilient, and futureready solution. The proposed solution shall fully comply with the requirements specified in the RFP and support future business and technology needs of the Bank. 2. As part of the requirement gathering phase, the OEM/OEM authorized partner shall conduct workshops, discovery sessions, interviews, and discussions with the Bank's stakeholders and appointed consultants to understand business requirements, existing infrastructure & solutions, integrations, operational processes, and security requirements. 3. The OEM /OEM authorized partner shall review the Bank's existing IT, security, application, network, cloud, and infrastructure landscape and recommend an optimized target-state architecture leveraging both existing and proposed components wherever feasible. 4. The OEM /OEM authorized parrtner but not be limited to: a. Requirements elicitation and analysis	No Change, Please be guided by the RFP
323	61	7.6.2 System Design - Activities are to be performed by Respective solution OEM (supported by bidder)	7.6.2	System Design - Activities are to be performed by Respective solution OEM 1. The bidder and respective OEM shall be responsible for the end-to-end design, sizing, customization, configuration, integration, implementation, deployment, maintenance, and support of the proposed solution, including coordination with all associated OEMs, service providers, and stakeholders. 2. All proposed NextGEN SOC solutions shall support seamless interoperability, realtime integration, event sharing, correlation, orchestration, and automated response capabilities to enable unified security operations and minimize manual intervention. 3. The proposed solution shall be configurable and customizable to meet the Bank's functional, technical, operational, reporting, security, and compliance requirements. 4. The bidder and OEM shall design and implement a secure, scalable, resilient, and future-ready architecture based on the approved requirements, data flows, integrations, and operational needs of the Bank. 5. The bidder and OEM shall prepare and submit the following design documents for Bank approval: a. High-Level Design (HLD), including solution	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner System Design - Activities are to be performed by Respective solution OEM/OEM authorized partner (supported by bidder) 1. The bidder and respective OEM /OEM authorized partner shall be responsible for the end-to-end design, sizing, customization, configuration, integration, implementation, deployment, maintenance, and support of the proposed solution, including coordination with all associated OEMs, service providers, and stakeholders. 2. All proposed NextGEN SOC solutions shall support seamless interoperability, realtime integration, event sharing, correlation, orchestration, and automated response capabilities to enable unified security operations and minimize manual intervention. 3. The proposed solution shall be configurable and customizable to meet the Bank's functional, technical, operational, reporting, security, and compliance requirements. 4. The bidder and OEM/OEM authorized partner shall design and implement a secure, scalable, resilient, and future-ready architecture based on the approved requirements, data flows, integrations, and operational needs of the Bank. 5. The bidder and OEM/OEM authorized partner shall prepare and submit the following design documents for Bank approval: a. High-Level Design (HLD), including solution architecture, deployment architecture, integration architecture, and data flow	No Change, Please be guided by the RFP
324	61	7.6.3 Development and Installation - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.6.3	1. All installation, configuration, customization, testing, migration, integration, UAT, GoLive, and related implementation activities shall be performed from the Bank's premises. 2. The bidder and respective OEM shall integrate the proposed solution with the Bank's ITSM, SLA Monitoring, monitoring, logging, authentication, and other enterprise platforms, as required. 3. The bidder and OEM shall coordinate with all relevant third parties, OEMs, service providers, and Bank stakeholders to ensure seamless integration, interoperability, and end-to-end functionality of the proposed solution. 4. The bidder shall provide all required integrations, connectors, parsers, APIs, workflows, playbooks, dashboards, reports, alerts, fine-tuning, customizations, enhancements, and remediation activities necessary for successful operation of the solution throughout the contract period without any additional cost to the Bank. 5. The bidder shall adopt and submit an implementation methodology covering solution deployment, customization, testing, managed services, facility management services, knowledge transfer, and hardware/software installation and configuration activities.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Development and Installation - Activities are to be performed by Respective Solution OEM /OEM authorized partner(supported by bidder) 1. All installation, configuration, customization, testing, migration, integration, UAT, GoLive, and related implementation activities shall be performed from the Bank's premises. 2. The bidder and respective OEM/OEM authorized partner shall integrate the proposed solution with the Bank's ITSM, SLA Monitoring, monitoring, logging, authentication, and other enterprise platforms, as required. 3. The bidder and OEM /OEM authorized partner shall coordinate with all relevant third parties, OEMs, service providers, and Bank stakeholders to ensure seamless integration, interoperability, and end-to-end functionality of the proposed solution. 4. The bidder shall provide all required integrations, connectors, parsers, APIs, workflows, playbooks, dashboards, reports, alerts, fine-tuning, customizations, enhancements, and remediation activities necessary for successful operation of the solution throughout the contract period without any additional cost to the Bank. 5. The bidder shall adopt and submit an implementation methodology covering solution deployment, customization,	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
325	62	7.6.4 Documentation - Activities are to be performed by Respective solution OEM (supported by bidder	7.6.4	The bidder and respective OEM shall prepare, maintain, obtain Bank approval/sign-off, and submit all project, technical, operational, security, and administrative documentation associated with the proposed solution. The indicative list of deliverables shall include, but not be limited to, the following: 1. Detailed Project Plan and Implementation Plan 2. Hardware, Software, Infrastructure, and Sizing Specifications 3. High-Level Design (HLD) and Low-Level Design (LLD) Documents 4. Solution Architecture, Deployment Architecture, and Data Flow Documents 5. Secure Configuration Standards, Baseline Hardening Documents, and Security Configuration Guides 6. System, Database, Integration, Troubleshooting, Diagnostics, and Maintenance Documents 7. Testing, Validation, Acceptance, and Go-Live Documents 8. Change Management, Release Management, Problem Management, and Operational Procedures 9. User Management, Access Management, and Role Administration Guides 10. Release Notes, Impact Assessment Matrix, and Dependency Mapping Documents	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Documentation - Activities are to be performed by Respective solution OEM/OEM authorized partner (supported by bidder The bidder and respective OEM shall prepare, maintain, obtain Bank approval/sign-off, and submit all project, technical, operational, security, and administrative documentation associated with the proposed solution. The indicative list of deliverables shall include, but not be limited to, the following: 1. Detailed Project Plan and Implementation Plan 2. Hardware, Software, Infrastructure, and Sizing Specifications 3. High-Level Design (HLD) and Low-Level Design (LLD) Documents 4. Solution Architecture, Deployment Architecture, and Data Flow Documents 5. Secure Configuration Standards, Baseline Hardening Documents, and Security Configuration Guides 6. System, Database, Integration, Troubleshooting, Diagnostics, and Maintenance Documents 7. Testing, Validation, Acceptance, and Go-Live Documents 8. Change Management, Release Management, Problem Management, and Operational Procedures 9. User Management, Access Management, and Role Administration Guides 10. Release Notes, Impact Assessment Matrix, and Dependency	No Change, Please be guided by the RFP
326	63	7.6.5 Deployment and Go-Live - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.6.5	1. The bidder and respective OEM shall be responsible for deployment of the solution in the production environment, Go-Live planning, implementation, installation, configuration, fine-tuning, migration, stabilization, and hyper care support. 2. The bidder and OEM shall provide onsite support during the hyper care period, monitor solution performance, assist users, conduct training sessions, address issues and defects, implement corrective actions, and recommend operational best practices. 3. The implementation scope shall include deployment planning, migration, testing, validation, issue resolution, user acceptance support, Go-Live execution, and postGo-Live stabilization activities. 4. Prior to Go-Live, the solution shall undergo security validation activities, including VAPT, IS Audit, readiness assessments, identification of security gaps and blind spots, risk remediation, and implementation of recommendations. The Bank or its appointed agency may conduct Continuous Automated Red Teaming, Purple Teaming, security assessments, or other validation exercises as deemed necessary. 5. The bidder and OEM shall conduct performance testing prior to UAT and Go-Live to validate that the	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Deployment and Go-Live - Activities are to be performed by Respective Solution OEM /OEM authorized partner (supported by bidder) 1. The bidder and respective OEM/OEM authorized partner shall be responsible for deployment of the solution in the production environment, Go-Live planning, implementation, installation, configuration, fine-tuning, migration, stabilization, and hyper care support. 2. The bidder and OEM /OEM authorized partner shall provide onsite support during the hyper care period, monitor solution performance, assist users, conduct training sessions, address issues and defects, implement corrective actions, and recommend operational best practices. 3. The implementation scope shall include deployment planning, migration, testing, validation, issue resolution, user acceptance support, Go-Live execution, and postGo-Live stabilization activities. 4. Prior to Go-Live, the solution shall undergo security validation activities, including VAPT, IS Audit, readiness assessments, identification of security gaps and blind spots, risk remediation, and implementation of recommendations. The Bank or its appointed agency may conduct Continuous Automated Red Teaming, Purple Teaming, security assessments,	Please refer addendum for revised clause
327	64	7.6.6 Testing- Activities are to be performed by Respective solution OEM (supported by bidder)	7.6.6	1. The Bank shall conduct User Acceptance Testing (UAT) to validate that the proposed solution and all associated components, integrations, workflows, reports, dashboards, and functionalities comply with the requirements specified in the RFP, approved FRSM/SRS, and other project documents. 2. The bidder and respective OEM shall confirm completion of all implementations, configuration, customization, integration, migration, and testing activities prior to commencement of UAT and certify that the solution is ready for user validation. 3. The bidder shall provision and maintain dedicated Development, Testing, UAT, and Pre-Production environments throughout the contract period. All software, licenses, and other resources required for such environments shall be included within the bidder's scope without any additional cost to the Bank. 4. Any defects, deviations, vulnerabilities, observations, or non-compliances identified during UAT, security assessments, audits, reviews, or validation exercises shall be rectified by the bidder within the timelines prescribed by the Bank and at no additional cost. 5. The bidder shall maintain appropriate version control, configuration management, change	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Testing- Activities are to be performed by Respective solution OEM/OEM authorized partner (supported by bidder) 1. The Bank shall conduct User Acceptance Testing (UAT) to validate that the proposed solution and all associated components, integrations, workflows, reports, dashboards, and functionalities comply with the requirements specified in the RFP, approved FRSM/SRS, and other project documents. 2. The bidder and respective OEM /OEM authorized partner shall confirm completion of all implementations, configuration, customization, integration, migration, and testing activities prior to commencement of UAT and certify that the solution is ready for user validation. 3. The bidder shall provision and maintain dedicated Development, Testing, UAT, and Pre-Production environments throughout the contract period. All software, licenses, and other resources required for such environments shall be included within the bidder's scope without any additional cost to the Bank. 4. Any defects, deviations, vulnerabilities, observations, or non-compliances identified during UAT, security assessments, audits, reviews, or validation exercises shall be rectified by the bidder within the timelines prescribed by the Bank and at no additional cost.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
328	65	7.6.6.1 Quality Assurance	7.6.6.1	1. Testing Requirements a. The respective OEM shall be responsible for planning, executing, documenting, and successfully completing all testing activities required to validate the functionality, performance, stability, reliability, security, interoperability, and operational readiness of the proposed solution. The bidder shall prepare detailed test plans, test cases, test data, automation scripts (where applicable), entry and exit criteria, test reports, defect logs, root cause analysis reports, workarounds, and remediation plans, and shall obtain the Bank's approval wherever required. 2. Test Preparation The respective OEM shall: a. Prepare the overall testing strategy and methodology for Unit Testing (UT), UAT, Performance Testing, Security Testing, and other applicable tests. b. Establish and maintain the required test environments, infrastructure, software, applications, and test data. c. Prepare, validate, and execute test cases, scripts, and automation frameworks, wherever applicable. d. Define test entry and exit criteria, acceptance criteria, and success parameters. 3. Test Execution The respective OEM shall: a. Execute all approved test cases and scripts. b. Record, track, report, and resolve defects,	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: 1. Testing Requirements a. The respective OEM/OEM authorized partner shall be responsible for planning, executing, documenting, and successfully completing all testing activities required to validate the functionality, performance, stability, reliability, security, interoperability, and operational readiness of the proposed solution. The bidder shall prepare detailed test plans, test cases, test data, automation scripts (where applicable), entry and exit criteria, test reports, defect logs, root cause analysis reports, workarounds, and remediation plans, and shall obtain the Bank's approval wherever required. 2. Test Preparation The respective OEM /OEM authorized partner shall: a. Prepare the overall testing strategy and methodology for Unit Testing (UT), UAT, Performance Testing, Security Testing, and other applicable tests. b. Establish and maintain the required test environments, infrastructure, software, applications, and test data. c. Prepare, validate, and execute test cases, scripts, and automation frameworks, wherever applicable. d. Define test entry and exit criteria, acceptance criteria, and success parameters. 3. Test Execution The respective OEM /OEM authorized partner	No Change, Please be guided by the RFP
329	66	7.6.7 Training- Activities are to be performed by Respective solution OEM (supported by bidder)	7.6.7	7.6.7 Training- Activities are to be performed by Respective solution OEM (supported by bidder) The bidder and respective OEMs shall provide comprehensive product training, knowledge transfer, and certification programs for the Bank's IT and Information Security personnel at no additional cost. All technical and product-specific training shall be delivered by OEM. Upon successful completion of the training programs, the respective OEM shall issue participation and/or certification certificates to the attendees. The bidder shall submit a detailed Training and Certification Plan covering training objectives, curriculum, skill levels, training schedules, participant eligibility, certification pathways, and assessment criteria. The training program shall cover product functionalities, administration, troubleshooting, maintenance, security best practices, automation, advanced threat scenarios, security monitoring and analysis, incident response and investigation, threat detection and hunting, intelligence analysis, new features, upgrades, operational workflows, and relevant industry trends. Bidder along with the OEM should provision the training & certification of the bank's relevant officials from the relevant Cloud service provider where the	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Training- Activities are to be performed by Respective solution OEM /OEM Authorized partner (supported by bidder) The bidder and respective OEMs /OEM authorized partner shall provide comprehensive product training, knowledge transfer, and certification programs for the Bank's IT and Information Security personnel at no additional cost. All technical and product-specific training shall be delivered by OEM/OEM Authorized partner. Upon successful completion of the training programs, the respective OEM /OEM Authorized partner shall issue participation and/or certification certificates to the attendees. The bidder shall submit a detailed Training and Certification Plan covering training objectives, curriculum, skill levels, training schedules, participant eligibility, certification pathways, and assessment criteria. The training program shall cover product functionalities, administration, troubleshooting, maintenance, security best practices, automation, advanced threat scenarios, security monitoring and analysis, incident response and investigation, threat detection and hunting, intelligence analysis, new features, upgrades, operational workflows, and relevant industry trends. Bidder along with the OEM/OEM authorized partner should provision the training & certification of the bank's relevant officials from the relevant	Please refer addendum for revised clause
330	67	7.6.8 Security requirements - Activities are to be performed by Respective solution OEM (supported by bidder)	7.6.8	1. The bidder and respective OEMs shall comply with the Bank's IT, Information Security, Cyber Security, Data Protection, Privacy, Business Continuity, and related policies, standards, procedures, and guidelines, as shared by the Bank from time to time. The bidder shall be responsible for ensuring the confidentiality, integrity, availability, security, and privacy of the Bank's information assets, systems, applications, and data throughout the contract period. 2. The bidder shall implement and maintain appropriate administrative, technical, physical, and operational controls for protection of data, applications, systems, infrastructure, and associated assets under its custody or management. 3. The bidder shall comply with the Bank's requirements relating to access management, privileged access management, password policies, user administration, data protection, encryption, monitoring, incident management, and security governance. 4. The bidder shall ensure encryption and protection of data at rest, data in transit, and data in use, wherever applicable, using industry-standard security controls and cryptographic mechanisms. All tools, technologies, and controls required to achieve the same shall form part of the proposed solution.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Security requirements - Activities are to be performed by Respective solution OEM/OEM authorized partner (supported by bidder) 1. The bidder and respective OEMs/OEM authorized partner shall comply with the Bank's IT, Information Security, Cyber Security, Data Protection, Privacy, Business Continuity, and related policies, standards, procedures, and guidelines, as shared by the Bank from time to time. The bidder shall be responsible for ensuring the confidentiality, integrity, availability, security, and privacy of the Bank's information assets, systems, applications, and data throughout the contract period. 2. The bidder shall implement and maintain appropriate administrative, technical, physical, and operational controls for protection of data, applications, systems, infrastructure, and associated assets under its custody or management. 3. The bidder shall comply with the Bank's requirements relating to access management, privileged access management, password policies, user administration, data protection, encryption, monitoring, incident management, and security governance. 4. The bidder shall ensure encryption and protection of data at rest, data in transit, and data in use, wherever applicable, using	No Change, Please be guided by the RFP
331	70	7.7 On-cloud proposed solution OEM Responsibilities	7.6.9	1. The security telemetry received by the OEM Cloud platform will be routed to the dedicated tenant/workspace provisioned for the Bank.	What is the requirement here, is it required to maintain a copy of all cloud data to a local instance /data lake, please clarify, who need to provision this, does bank has this instance available, if not required please remove this ask.	The security telemetry received and processed by the OEM Cloud/SaaS platform shall be logically segregated and maintained within a dedicated tenant/workspace provisioned for the Bank. The dedicated tenant/workspace shall ensure segregation of the Bank's security data, configurations, policies, analytics, alerts, incidents and other Bank-related information from those of other customers.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
332	71	7.10 Data Privacy	7.1 0	Executive Governance and Project Oversight 1. The bidder and each respective OEM shall nominate a senior executive as the Project Sponsor/Project Director responsible for executive governance, stakeholder management, escalation management, strategic oversight, and overall project success. 2. The Project Sponsor, Project Director, and designated senior representatives of the bidder and OEMs shall participate in governance meetings, executive reviews, strategy workshops, and escalation meetings as required by the Bank. An, On quarterly/or as per the frequency defined by bank, executive governance meetings shall be conducted throughout the contract period to review project progress, service delivery, operational performance, security posture, compliance, risks, technology enhancements, and continuous improvement opportunities. 3. The bidder and OEMs shall deploy and maintain adequately skilled, certified, experienced, and qualified resources, together with appropriate backup resources, succession planning, and skill development mechanisms, to ensure uninterrupted 24x7x365 service delivery throughout the contract period.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Executive Governance and Project Oversight 1. The bidder and each respective OEM/OEM authorized partner shall nominate a senior executive as the Project Sponsor/Project Director responsible for executive governance, stakeholder management, escalation management, strategic oversight, and overall project success. 2. The Project Sponsor, Project Director, and designated senior representatives of the bidder and OEMs /OEM authorized partner shall participate in governance meetings, executive reviews, strategy workshops, and escalation meetings as required by the Bank. An, On quarterly/or as per the frequency defined by bank, executive governance meetings shall be conducted throughout the contract period to review project progress, service delivery, operational performance, security posture, compliance, risks, technology enhancements, and continuous improvement opportunities. 3. The bidder and OEMs /OEM Authorized partner shall deploy and maintain adequately skilled, certified, experienced, and qualified resources, together with appropriate backup resources, succession planning, and skill development mechanisms, to ensure uninterrupted 24x7x365 service delivery throughout the contract period. 4. The bidder shall establish and maintain a Bank-approved	Please refer addendum for revised clause
333	72	7.12 Resource Requirement	7.6.12	7.12.1Implementation Phase • Prior to commencement of implementation, the bidder and respective OEMs shall submit a detailed Resource Deployment Plan for Bank approval identifying proposed onsite and offsite resources, roles, responsibilities, certifications, experience, deployment schedules, and solution-wise allocation. • The bidder shall deploy a dedicated onsite Project Manager throughout the implementation phase and nominate appropriate bidder and OEM resources for each solution, workstream, milestone, and project activity. • Any replacement, redeployment, or modification of approved implementation resources shall require prior written approval from the Bank.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Implementation Phase • Prior to commencement of implementation, the bidder and respective OEMs /OEM authorized partner shall submit a detailed Resource Deployment Plan for Bank approval identifying proposed onsite and offsite resources, roles, responsibilities, certifications, experience, deployment schedules, and solution-wise allocation. • The bidder shall deploy a dedicated onsite Project Manager throughout the implementation phase and nominate appropriate bidder and OEM /OEM authorized partner resources for each solution, workstream, milestone, and project activity. • Any replacement, redeployment, or modification of approved implementation resources shall require prior written approval from the Bank.	No Change, Please be guided by the RFP
334	72	7.12.2Operations and Maintenance (O&M) Phase		7.12.2Operations and Maintenance (O&M) Phase • The bidder shall deploy the minimum onsite L1, L2, Project Manager/L3 – Operations, and other resources specified in the RFP and ensure uninterrupted 24x7x365 support through an appropriate shift-based deployment model. • The respective OEMs shall provide subject matter experts from the date of installation throughout the contract period to support operations, troubleshooting, optimization, upgrades, audits, vulnerability remediation, and major incidents. • The bidder shall ensure adequate SME support for timely resolution of incidents, service requests, problems, vulnerabilities, and operational issues.	O & M shall be bidders responsibility pleaase remove OEM from this to maintain right availability and cost Operations and Maintenance (O&M) Phase • The bidder shall deploy the minimum onsite L1, L2, Project Manager/L3 – Operations, and other resources specified in the RFP and ensure uninterrupted 24x7x365 support through an appropriate shift-based deployment model. • The respective bidder shall provide subject matter experts from the date of installation throughout the contract period to support operations, troubleshooting, optimization, upgrades, audits, vulnerability remediation, and major incidents. • The bidder shall ensure adequate SME support for timely resolution of incidents, service requests, problems, vulnerabilities, and operational issues.	No Change, Please be guided by the RFP
335	73	7.12.3Resource Management and Governance	7.12	OEM Implementation Resources Onsite (Full Time) OEM shall submit a detailed resource deployment plan before commencement of requirement gathering. Any replacement or modification shall require prior Bank approval.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: OEM /OEM authorized partner Implementation Resources Onsite (Full Time) OEM/OEM authorized partner shall submit a detailed resource deployment plan before commencement of requirement gathering. Any replacement or modification shall require prior Bank approval.	No Change, Please be guided by the RFP
336		7.17 System recovery	1	. In case of disaster, it is the responsibility of the Respective solution OEM along with the bidder to ensure that services remain unaffected and same is up and running from secondary site (DR)	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: . In case of disaster, it is the responsibility of the Respective solution OEM/OEM Authorized partner along with the bidder to ensure that services remain unaffected and same is up and running from secondary site (DR)	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
337		7.19 Other In-Scope Services	7.19	7.19.1Other Scope Activity 1. The Respective solution OEM along with the bidder is expected to ensure that all functionalities as mentioned in Appendix 1A: Functional Specification are made available to PSB. 2. The Respective solution OEM along with the bidder is expected to ensure that for the purpose of this RFP, statutory and regulatory changes shall mean any change prescribed by the statutory and regulatory bodies governing/ affecting the banking industry in India viz. Reserve Bank of India, Ministry of Finance, CCIL, NPCI, IBA, SEBI, or any such bodies constituted by the RBI mandating change/s to an existing functionality of the Solution shall be provided to the Bank at no additional cost for the entire contract period. However, any Statutory and Regulatory changes post Go-Live of the respective applications (which are not a part of the existing functionalities) will be on CR basis based on the rates provided in the Bill of Material. 3. The Respective Solution OEM along with the bidder is expected to carry out a requirement study for the functionalities and services required by PSB, to gain understanding of the business requirements. 4. Respective solution OEM along with the bidder	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: 1Other Scope Activity 1. The Respective solution OEM/OEM Authorized partner along with the bidder is expected to ensure that all functionalities as mentioned in Appendix 1A: Functional Specification are made available to PSB. 2. The Respective solution OEM/OEM Authorized partner along with the bidder is expected to ensure that for the purpose of this RFP, statutory and regulatory changes shall mean any change prescribed by the statutory and regulatory bodies governing/ affecting the banking industry in India viz. Reserve Bank of India, Ministry of Finance, CCIL, NPCI, IBA, SEBI, or any such bodies constituted by the RBI mandating change/s to an existing functionality of the Solution shall be provided to the Bank at no additional cost for the entire contract period. However, any Statutory and Regulatory changes post Go-Live of the respective applications (which are not a part of the existing functionalities) will be on CR basis based on the rates provided in the Bill of Material. 3. The Respective Solution OEM/OEM Authorized partner along with the bidder is expected to carry out a requirement study for the functionalities and services required by PSB, to gain understanding of the business requirements. 4. Respective solution OEM /OEM Authorized partner along	Please refer addendum for revised clause
338		7.19.4DR Setup - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.19.4	DR Setup - Activities are to be performed by Respective Solution OEM (supported by bidder) 1. Respective solution OEM along with the bidder has to ensure that DR setup is ready on the date of Go Live of respective Applications 2. Respective solution OEM along with the bidder should make necessary setup to enable the DR within the agreed timelines. 3. Respective solution OEM along with the bidder should carry out the deployment of the application in DC and DR, UAT as applicable. 4. To ensure proper rollback, Respective solution OEM along with the bidder has to ensure that the old setup at all the locations is as–IS as per the agreed timelines during migration strategy formulation	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner DR Setup - Activities are to be performed by Respective Solution OEM /OEM authorized partner (supported by bidder) 1. Respective solution OEM /OEM Authorized partneralong with the bidder has to ensure that DR setup is ready on the date of Go Live of respective Applications 2. Respective solution OEM/OEM Authorized partner along with the bidder should make necessary setup to enable the DR within the agreed timelines. 3. Respective solution OEM/OEM Authrized partner along with the bidder should carry out the deployment of the application in DC and DR, UAT as applicable. 4. To ensure proper rollback, Respective solution OEM/OEM Authrized partner along with the bidder has to ensure that the old setup at all the locations is as–IS as per the agreed timelines during migration strategy formulation	No Change, Please be guided by the RFP
339		13 SERVICE LEVELS & PENALTIES	2	2. The bidder and the OEM shall be jointly responsible for the maintenance, configuration, performance, and fault-free operation of the entire supplied infrastructure, including hardware, software, operating systems, databases, and related components, during the warranty, AMC, ATS, and FMS periods, as applicable	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: The bidder and the OEM /OEM authorized partner shall be jointly responsible for the maintenance, configuration, performance, and fault-free operation of the entire supplied infrastructure, including hardware, software, operating systems, databases, and related components, during the warranty, AMC, ATS, and FMS periods, as applicable	No Change, Please be guided by the RFP
340	159	14.1 Assignment & Subcontracting	1	The selected bidder shall not subcontract/JV/Consortium or permit anyone to perform any of the work, service or other performance required under the contract (excluding Proposed OEM personnels). All bidder's personnel proposed for the bank shall be on bidder's Payroll. Bank will seek relevant documentation from the bidder to validate the same.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: The selected bidder shall not subcontract/JV/Consortium or permit anyone to perform any of the work, service or other performance required under the contract (excluding Proposed OEM /OEM Autorized partner personnels). All bidder's personnel proposed for the bank shall be on bidder's Payroll. Bank will seek relevant documentation from the bidder to validate the same.	No Change, Please be guided by the RFP
341	117	10.2	Eligibility Criteria-Clause-22	The proposed OEM solution should have been implemented in at least one verifiable client in India. Credential is to be submitted for the following solutions: a. CNAPP b. CWPP c. CTEM	CTEM is a new framework and customers are still in evaluation/ Implementation phase. Suggested change Client in India or Global BFSI The proposed OEM solution should have been implemented in verifiable client in India or Global. Credential is to be submitted for each of the following solutions: 1. CNAPP 2. CWPP 3. CTEM	No Change, Please be guided by the RFP
342	120	10.2	Eligibility Criteria-Clause-23	The proposed OEM services should have been implemented in at least one (1) PSU/ PSE/ Government Organizations / BFSI in India. Credential is to be submitted for the following services: 1. Breach Attack & Simulation 2. Continuous Automated Red Teaming 3. Attack surface management 4. Phishing simulation 5. Anti-phishing services 6. Dark web monitoring 7. Brand protection & monitoring 8. Threat Intelligence feed 9. Threat Hunting services	As the offsite services are specified under the functional compliance requirements and are expected to be provided by the bidder, the corresponding eligibility criteria should be assessed at the bidder level. Suggested Changes: The proposed bidder services (below mentioned to the services) should have been implemented by the bidder in in at least one verifiable client in India.	No Change, Please be guided by the RFP
343	86	16	Technical Specs-Anti Phishing-	Solution must be able to seamlessly integrate with On-Prem Mail Gateways via Mail Transfer Agent (MTA) forwarding	Anti-Phishing is asked as a Managed service however MTA is a componentfor onprim SEG gateway Suggested Change: Solution must be able to seamlessly integrate with On-Prem Mail Gateways via API integration	Please refer to the relevant Addendum for updated specfications
344	87	18.2	Technical Specs-Anti Phishing-	Solution must provide DoS protection and directory harvest attack protection to ensure the availability of email services	DOS Protection Is Typically the Responsibility of the hardware based Email Infrastructure or Secure Email Gateway or Firewall or dedicated DDOS protection Hence this clause should not fall under Anti-Phishing services Also, this feature Suggested Change: Remove this clause	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
345	87	19.2	Technical Specs-Anti Phishing	Solution must be able to display HTML banners on email clients, automatically switching to plain text format if HTML is not supported, while also providing multilingual support based on the organization's language preferences. HTML banner content can be edited or customized by organization	The requirement appears to prescribe a specific notification mechanism (HTML banner insertion) rather than the intended security outcome of user awareness and phishing risk notification. Modern anti-phishing solutions may provide user alerts through native email client warnings, subject tagging, security indicators, API-based notifications, or other mechanisms without relying on HTML banner injection. Suggested Change: Remove the clause	Please refer to the relevant Addendum for updated specfications
346	87	19.4	Technical Specs-Anti Phishing	Solution must offer multiple disposition options, including attachment stripping, delivery of notices to senders, and quarantine of the whole email	Delivery of notice is platform specific feature Suggested Change Solution must offer multiple disposition options, including attachment stripping, and quarantine of the whole email	Please refer to the relevant Addendum for updated specfications
347	87	19.5	Technical Specs-Anti Phishing	Solution must provide a "Safe Preview" capability for administrators to view detailed information of quarantined messages and decide necessary actions	Safe Preview is a broad term, it should relate to anti-phishing Suggested Change Solution must provide a "Safe Preview of links" capability for administrators to view detailed information of quarantined messages and decide necessary actions	Please refer to the relevant Addendum for updated specfications
348	88	19.8	Technical Specs-Anti Phishing-	As part of the forensic collection, should include the capture of PowerShell history	The requirement appears to mandate a specific forensic artefact (PowerShell history) rather than the intended security objective of investigating PowerShell-based activity. Suggested Change As part of the forensic collection, should include the capture of PowerShell history or equivalent forensic mechanism	Please refer to the relevant Addendum for updated specfications
349	88	19.17	Technical Specs-Anti Phishing-	Solution must provide detailed reporting covering system usage and other areas including global message summary, spam, virus and other rule actions to save administrator time and effort in the collection of data for status reports. Reports can be emailed (HTML), printed, or downloaded in CSV format for use with third party tools	Suggested Changes: Solution must provide detailed reporting covering system usage and other areas including global message summary, spam, virus and other rule actions to save administrator time and effort in the collection of data for status reports. Reports can be emailed (HTML), printed, or downloaded in CSV or PDF format for use with third party tools	Please refer to the relevant Addendum for updated specfications
350	88	19.18	Technical Specs-Anti Phishing-	Solution must have capability for administrators to view reports containing detailed statistics covering emails processed, rejected emails, SMTP transactions, and communication flows	The requirement mandates visibility into SMTP transactions and communication flow analytics, which are traditionally functions of MTA,and may not have direct access in API-based or cloud-native anti-phishing solutions. Suggested Change Solution must have capability for administrators to view reports containing detailed statistics covering emails processed, rejected emails.	Please refer to the relevant Addendum for updated specfications
351	89	19.37	Technical Specs-Anti Phishing-	Solution must support message classification management, including separate classifiers for spam, impersonation, bulk, phishing, adult, and malware messages, with the ability to set score thresholds per category.	The requirement mandates a specific detection architecture based on separate classifiers and per-category scoring thresholds. Modern email security and anti-phishing solutions increasingly leverage AI/ML models, behavioural analytics, graph intelligence, and composite risk engines that may not expose individual classifiers Suggested Change Solution must support message classification management, including separate classifiers for spam, impersonation, bulk, phishing and malware messages, with the ability to set score thresholds per category.	Please refer to the relevant Addendum for updated specfications
352	89	19.41	Technical Specs-Anti Phishing	Solution must provide granular administrative controls to allow role-based access to each module and quarantine folder.	Modern cloud-native anti-phishing solutions implement administrative segregation through configurable RBAC, delegated administration, role groups, and permission-based access models, which may not necessarily expose permissions at the individual module or quarantine-folder level Suggested Change Solution must provide granular administrative controls to allow role-based access	Please refer to the relevant Addendum for updated specfications
353	89	19.43	Technical Specs-Anti Phishing	Solution must support complicated mail routing requirements, including group-based routing based on user groups	The requirement appears to address email infrastructure and mail-flow routing capabilities rather than core anti-phishing or email threat protection functionality. Complex mail routing, transport rules, and group-based routing are typically implemented within the email platform Suggested Change Remove this clause, its not applicable	Please refer to the relevant Addendum for updated specfications
354	89	19.5 0	Technical Specs-Anti Phishing	solution must support a range of routing behaviors and actions for different scenarios, allowing administrators to customize email handling based on specific needs and requirements.	The requirement is broad and appears to focus on email routing and mail-flow management capabilities, which are typically functions of the email infrastructure (Microsoft Exchange, Exchange Online Suggested Change Remove this clause, its not applicable	Please refer to the relevant Addendum for updated specfications
355	90	19.51	Technical Specs-Anti Phishing	Solution must support for in outbound or inbound email including footer management Inserting one or more legal or compliance footers (e.g. disclaimer) Multi-language support Apply different filters based on email attributes or active directory attributes, Insert dynamic content to footer such as date, when to apply the footer in the message routing hops, Selectively apply based on policy / attribute or not apply if the email is s/mime encrypted or digitally signed, etc Apply signatures and disclaimers based on AD user groups	Footer management is vendor specific feature Suggested Change Remove the clause	Please refer to the relevant Addendum for updated specfications
356	90	19.5 3	Technical Specs-Anti Phishing	Solution must allow end-users to receive customized email notifications based on domain name.	The clause prescribes a specific notification customization method (domain-based) that may not be supported by all modern cloud-native Anti-Phishing solution Suggested Change: Solution must allow end-users to receive customized email notifications based alerts, and awareness messages based on organizational policies	Please refer to the relevant Addendum for updated specfications
357	90	19.5 7	Technical Specs-Anti Phishing	Solution must provide administrators with capabilities for email queue management	This feature is excahnge or onprim gateway specific. Suggested Change Remove the clause	Please refer to the relevant Addendum for updated specfications
358	90	19.5 9	Technical Specs-Anti Phishing	Solution must support alerting the security team on all policies, quarantine folders, and queue thresholds	The clause is a gateway-specific alerting model based on quarantine folders and queue thresholds. Modern cloud-native email security solutions may not utilise traditional mail queues while still providing comprehensive alerting for security incidents, policy actions, quarantine events, and operational status Suggested Change Solution must support alerting the security team on all policies, quarantine folders, and queue thresholds or equivalent alerting mechanism	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
359	90	19.6 2	Technical Specs-Anti Phishing	Solution must provide application and message routing troubleshooting tools with a message-tracing capability to facilitate help desk work	Message routing trobleshooting & message-tracing capabilities are part of exchange provider. Suggested Change Remove the clause	Please refer to the relevant Addendum for updated specfications
360		Appendix 1A Functional Compliance Sheet (Solutions) CTEM	8	The solution should allow messaging and collaboration within the context of a specific intelligence item	We understand that this scope is for the bidder to collaborate on incidents/alerts within the team.	Please refer the below clarification: Example: CVE is found in multiple endpoints/devices then it should be contextualized and integrate with SIEM for Incident creation The System should provide access to relevant team and share RBAC intelligence
361			24	The solution should provide pre-built bidirectional integrations with SIEM, SOAR, ticketing (Manage Engine), and threat intelligence platforms	We understand that the bidder will share the data with various on-premises tools like SIEM, SOAR, and ticketing tools (ManageEngine); hope this meets your requirement.	Please refer addendum for revised clause
362			31	The solution should display a Security Score overview with full breakdown by issue category	Can the bidder provide the risk rating of the organization? We hope this will suffice the requirement.	Yes, Solution Need to provide Risk Rating on the Infrastructure.
363			CTEM item 35	The solution should detect malicious files, reconnaissance activity, automated attack tools, and target lists	We understand that the bidder can achieve this functional requirement using a combination of tools like SIEM, SOAR, and other SOC components.	Please refer addendum for revised clause
364			43	The ML model should continuously study the environment including asset relationships, topology, and security controls to detect false positives and identify root causes	We understand that the bidder can achieve this functional requirement using a combination of tools like SIEM, SOAR, UEBA, and other SOC components like TIP or EDR.	Yes, Understanding is correct
365			48	The solution should assess and harden network, endpoint, and operating system security controls	We understand that the bidder can achieve this functional requirement using a combination of tools like SIEM, SOAR, UEBA, and other SOC components like TIP or EDR, including the day-to-day operations of SOC analysts.	Please refer addendum for the revised clause
366			51	The solution should apply virtual patching/compensating controls/exposure mitigation mechaism to the firewall and other security systems through integration with relevant security controls.	We understand that the bidder can take preventive measures on other solutions, either manually or automatically using SOAR, based on the findings received from the CTEM solution.	Please refer addendum for the revised clause
367			62	The solution should leverage compensating controls and layered defense strategies to manage threats proactively	We understand that this requirement can be achieved by the bidder through analysts managing the SOC during their day-to-day operations.	Please refer addendum for revised clause
368		Appendix 1A Functional Compliance Sheet (Services) ASM	3	Solution should store historical information about bank to provide cybersecurity maturity over time	We understand that bank requires solution to store a detailed/ historical information on the detections and the attacks which were targeted on during the complete contract duration.	Yes, Your understanding is correct
369			24	The solution must allow the organization to define the prioritization of assets based upon impact of the asset	We undestand that bank requires special attention/priortization to specific assests, so the bank can take preventive measures/ obseravility on it, it may be like assigning tags to certain important tags and creating a dashboard for critical ones.	Yes, your understanding is correct
370			26	Solution must provide a workflow to define and manage state of discovered entities which affects the priority of the entity.	We understand that bank requires the solution to enable workflow for alerting the adminsitrators for any vulnerability detection on the discovered critical assests.	Yes, your understanding is correct
371			35	Solution should have the feature to automatically create help desk ticket containing asset meta data, comments, link back to the solution console and guidance. Ticket status should be automatically reflected in ASM console.	Please amend the clause as: Solution should have the feature to automatically create help desk ticket containing asset meta data, comments, link back to the solution console and guidance. Justification: We want authorities to clarify this, as we understand that bank requires ASM console to create tickets automatically for the detections and analysts to work upon?	Please refer addendum for the revised clause
372			38	Solution must have bi-directional, writetable API's that allow the organization to integrate data into the organization's existing security	Please amend the clause as: Solution must have API's that allow the organization to integrate data into the organization's existing security Justification: since its services scope which is used to provide the outside attack surface details not the TIP Functionality so bidirectional API are not part of it.	Please refer addendum for the revised clause
373		Appendix 1A Functional Compliance Sheet (Services) Brand Abuse	25	The Bidder should provide for identification of fake recruitment schemes claiming affiliation with the Bank	We understand that bank requires solution to provide for identification of fake recruitment schemes claiming affiliation with the Bank which has the bank names and logo or any other identification method	Please refer addendum for revised clause
374			33	Search engines (like Google, yahoo, bing etc.) listing frauds where the customer care number & branch address of banks is changed/ modified should be continuously tracked and the same should be brought down immediately including True caller and JustDial.	Please delete this cluase its oem specific. Please modify the clause as to make it vendor neutral: Monitoring all major mobile app marketplaces for counterfeit, copycat apps, or apps infringing trademarks	Please refer addendum for the revised clause
375			37	Bidder should be able to identify and report to the bank if access to blocked ports on a webserver is sought by an external user.	We understand that the ask is not resticted to Brand abuse solution bidder can achive this requirenment with the combination of multiple solutions as it would also requires logs from perimeter and application security solutions, its is part of SIEM Solution.	Please refer addendum for the revised clause
376		Appendix 1A Functional Compliance Sheet (Services) Dark Web Monitoring	21	Monitor suspicious SSL/TLS certificate issuance.	We understand that bidder can achive this requirenement from either services product like ASM, Brand abuse or TI, this ask is not restrcited to DWM. As functional requirenment of bank is achieved anyways.	Yes, Understanding is correct
377			25	Provide Passive DNS intelligence and historical DNS resolution.	We understand that bank requires DNS intelligence and bank wants the bidder to store the historical logs/analysis of the DNS specific abuse.	Yes, your understanding is correct
378			40	Monitor C2 infrastructure, malware hosting, phishing infrastructure and botnets.	We undertand that bank requires information about the fake webistes which impersonating as PSB to Monitor C2 infrastructure, malware hosting and phishing infrastructure and botnets.	Yes, your understanding is correct

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
379			44	Support Email, SMS, and other notifications based on configurable severity.	We understand that bidder can achive this requirenment by combination of multiple products to achive this functionality spcifically ITSM.	Yes, your understanding is correct
380				clarifications	Please clarify: Does the solution have an established threat intelligence capability with more than 8 years of experience in global threat intelligence collection, analysis and threat actor tracking?	No Change, Please be guided by the RFP
381				clarifications	Please clarify: Does the solution leverage intelligence from a global network of 400+ threat researchers, analysts and threat hunters?	No Change, Please be guided by the RFP
382				clarifications	Please clarify: Does the solution collect and analyze threat intelligence across 14+ languages and sources?	No Change, Please be guided by the RFP
383				clarifications	Please clarify: Does the solution provide threat intelligence derived not only from network and publicly available sources, but also from active monitoring, engagement and communication with relevant threat actor groups and underground communities to identify planned attacks, emerging campaigns, TTPs, compromised assets and indicators of compromise?	No Change, Please be guided by the RFP
384				clarifications	Please clarify: Does the solution provide actionable threat intelligence on threat actor groups and campaigns, including their objectives, targeting, attack methods, TTPs, infrastructure and intended victims, along with recommended mitigation and protection measures to help the organization proactively defend against such threats?	No Change, Please be guided by the RFP
385		Appendix 1A Functional Compliance Sheet (Services) Threat Hunting	3	Create use-cases correlation rules specific to client's environment and event sources.	We understand that the bidder can achieve this functional requirement using a combination of tools like SIEM, SOAR, UEBA, and other SOC components like TIP or EDR, including the day-to-day operations of SOC analysts. OEM, Services do not directly perform detection engineering. We however provide recommendations on identified gaps in detections	No Change, Please be guided by the RFP
386			9	Review effectiveness of SOC to detect similar events..	We understand that the bidder can achieve this functional requirement using a combination of tools like SIEM, SOAR, UEBA, and other SOC components like TIP or EDR, including the day-to-day operations of SOC analysts. OEM, Services do not directly perform detection engineering. We however provide recommendations on identified gaps in detections	No Change, Please be guided by the RFP
387			13	Threat Hunting shall also address the following If the SOC has detected the attack, then identify the reasons for no action being taken if the SOC has not detected the attack, then identify if an existing correlation rule requires tuning or if a new correlation rule is required or if a new solution is required.	We understand that the bidder can achieve this functional requirement using a combination of tools like SIEM, SOAR, UEBA, and other SOC components like TIP or EDR, including the day-to-day operations of SOC analysts. OEM, Services do not directly perform detection engineering. We however provide recommendations on identified gaps in detections	No Change, Please be guided by the RFP
388				clarifications	Since RFP Ask for the Threat hunting servcies from OEM but does not define the no of hours: Please clarify that the solution should be sized on the below: Vendor shall propose a 200-hour package to start with along with per hour cost and Bank shall decide to extend the number of hours depending on scope expected	No Change, Please be guided by the RFP Refer Section 7.2.2 Services
389				clarifications	Please clarify: Does the proposed service provide organization-wide ransomware readiness and threat hunting across the complete security ecosystem, including infrastructure/products, people and processes, to proactively identify ransomware-related risks, vulnerabilities, attack paths, indicators and gaps, along with recommended remediation actions?	No Change, Please be guided by the RFP. The requirement shall be interpreted in accordance with the scope and functionalities specified under Section 7.4.8 – Threat Hunting Services, Appendix 1C. The Threat Hunting Service is intended to provide proactive, hypothesis-driven and intelligence-led technical threat hunting across the Bank's IT and security ecosystem. The service may utilize relevant telemetry and logs available through the Bank's SIEM, as well as other applicable security technologies and data sources, for identifying known and unknown threats,
390				clarifications	Please clarify: Does the proposed service provide a comprehensive maturity assessment with a defined maturity rating and actionable recommendations to strengthen the overall cybersecurity program, prioritize security initiatives and investments, and improve business continuity, resilience and recoverability during unexpected cyber incidents?	No Change, Please be guided by the RFP
391				clarifications	Please clarify: Does the proposed service provide a modular cybersecurity assessment and incident-readiness package offering, at a minimum, the following capabilities as per organizational requirements: SOC Gap Assessment, Ransomware Assessment, Forensic Analysis, Compromise Assessment, Incident Response Readiness Assessment, Active Directory Security Assessment, Tabletop Exercises, and Incident Response Playbook Development?	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
392		Appendix 1A Functional Compliance Sheet decoy	20	Includes an algorithm for automated rule creation that integrates with SOAR platforms, enabling real-time blocking of attacker IPs based on threat intelligence gathered from decoys. Features a customizable Generative AI model to assist security analysts with contextual insights, investigative support, and proactive security measures.	Please amend the clause as: Includes an algorithm for automated rule creation that integrates with SOAR platforms, enabling real-time blocking of attacker IPs based on threat intelligence gathered from decoys. Justification: GenAI is a functaionlity of soar solution where SOAR can create and run the playbook as per the event or alert where decoy is reponibsle for redirecting the attacker to fake vm to monitor the actvitites.	Please refer addendum for revised clause
393			25	The proposed solution shall be delivered as a cloud-based/SaaS platform hosted within the CSP environment. The bidder shall provision and size the required cloud compute, storage, network, and other platform resources to meet the Bank's performance, scalability, High Availability (HA), service continuity, and Disaster Recovery (DR) requirements in accordance with the applicable Cloud Deployment Model.	Please amend the clause as: Proposed Solution must cover complete scope of min of 200 applications, networks, devices with 50 segments across DC-DR and capability to add additional decoy connector through decoy customization as per requirement Justification: Request to amend the requirement to allow an on-premises Deception Solution instead of a cloud-based solution, as cloud-based redirection of decoy traffic may introduce latency and dependency on WAN/Internet connectivity, impacting real-time attacker engagement and the overall effectiveness of deception.	Please refer addendum for revised claus
394	1	Primary Storage	5	Proposed storage solution should be offerred with minimum 2 controllers with minimum 256 GB DRAM Cache memory on the entire storage Solution. The solution should scale to atleast 512GB Cache memory by adding additional controller.	Change To: Proposed storage solution should be offerred with minimum 2 controllers with minimum 128 GB DRAM Cache memory on the entire storage Solution. The solution should scale to atleast 256GB Cache memory by adding additional controller. Explaination: Cache ask should be Reduced as cache of 64GB or less per controller (128GB total) is enough as the latest CPUs, high-speed memory, and Gen 5 PCIe cards deliver the required performance efficiently. Modern storage controllers optimize cache usage, and industry benchmarks confirm that asked performance can be achieved with lower memory. This reduction not only meets technical needs but also decreases hardware, power, and cooling costs, resulting in a lower TCO for the solution	No Change, Please be guided by the RFP
395	1	Backup Solution	16	The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data over a secure, API-based disk-to- disk (D2D) connection.	Change To: The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data using standard Data protocolos such as FC, ISCI, NFS, S3 Expalination: This specific ask qulifies only specific backup appliance not any target storage as enterprise storage do not support data ingestion using API rather laverage protocols such as FC, ISCI, NFS, S3.	Please refer addendum for revised clause
396	1	Backup Solution	25	The Proposed Appliance/Backup Storage must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism	Change To:The Proposed Appliance/Backup Solution must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism Explaination: Proposed ask should be from Solution instead of storage as any storage does not offer file-level checksum reporting for backup files. This is typically a function of the backup software (e.g., Commvault, Veeam) that stores backups on storage.	Please refer addendum for revised clause
397	1	Primary Storage	21	If the OEM proposes effective storage capacity, then DRR should be applicable for the entire contract period. Incase, the DRR is not achieved anytime during the contract period, the OEM is liable to supply the additional drives/capacity to meet the required performance and effective capacity at no additional cost to the bank.	Query:Bank should provide workload details such as if data would encrypted or non-encrypeted, compressed or non-compressed and type of DB, VM etc. Explaniation: It would help OEM to size solution with correct DRR commitment.	Bidder/OEM shall assess the workload details and other relevant technical requirements and propose a suitably sized and architected solution meeting all requirements & terms of the RFP. The Bidder/OEM shall be responsible for sizing, performance, interoperability and adequacy of the proposed solution
398	1	Long Term Storage		Addititional Point Request	Point to be written as: Long Term Storage should support WORM (Wrte Once, Read Many) capability to have Data Immutability. Explaination: We recommend implementing WORM (Write Once, Read Many) capability for long-term backup storage to ensure data is protected against accidental deletion and ransomware attacks. Additionally, WORM functionality is required to comply with regulatory guidelines for banking institutions. Since backup storage is expected to provide WORM capability, long-term backup storage should also comply with this requirement to maintain robust data protection.	As per tender pg no. 39, point a, "No Bank data shall be deleted or made inaccessible before expiry of the applicable retention period (refer annexure 21) and without explicit written authorization from the Bank" It is bidders responsibility to ensure that they comply with the tender requirement
399	1	Primary Storage Backup Storage Long Term Storage		New Point request	Point to be written as: The proposed storage systems (for all 3 storage requirements), should have launch dates within past 3 years Explainations: We recommend qualifying storage systems with a launch date within the past three years. This approach ensures a better return on investment and reliable long-term support for a period of 7 to 10 years, as required by the bank. Some OEMs are currently offering systems that are over six years old and lack a clear roadmap or support commitment, which poses a risk to long-term operational stability and longitivity.	Please refer addendum for revised clause.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
400	50-52	Functional Requirements – Solutions	7.3.11 / 7.3.12 / 7.3.13	CSPM, CNAPP and CWPP requirements for cloud environments	Which cloud provider(s) are you predominantly using?	Details shall be shared with the successul bidder, the proposed solution should comply with the requirement mentioned in the RFP
401	29-34	Solution & Services Deployment Model	7.2 / 7.2.4	Solution deployment model and deployment architecture	Would you be requiring dedicated/100% isolated cloud SAAS tenant or shared cloud SAAS tenant?	Please refer addendum for the revised deployment architecture The security telemetry received and processed by the OEM Cloud/SaaS platform shall be logically segregated and
402	51-53	Functional Requirements – Solutions	7.3.12 / 7.3.13	CNAPP and CWPP requirements covering Kubernetes environments	Are you running Kubernetes workloads? If yes, are they managed or self-managed?	Details shall be shared with the successul bidder, the proposed solution should comply with the requirement mentioned in the RFP
403	52-53	Functional Requirements – Solutions	7.3.12 / 7.3.13	CNAPP/CWPP requirements for Kubernetes and runtime protection	Do you need Kubernetes Runtime security & enforcement as part of the CNAPP platform?	Details shall be shared with the successul bidder, the proposed solution should comply with the requirement mentioned in the RFP
404	51-52	Functional Requirements – Solutions	7.3.12.1, Point 4	API security findings shall be correlated with applications, cloud resources, workloads, identities and network resources	Do you need API security as well ? Which API Gateway are you using - cloud native service or self-hosted?	Bank currently is in process of implementing API Security, details of which shall be shared with the successul bidder, the proposed solution should comply with the requirement mentioned in the RFP
405	50	Functional Requirements – Solutions	7.3.11.1	CSPM shall provide centralized visibility across cloud assets and resources	Approximately how many cloud accounts/projects are in scope?	Details shall be discussed with the successful bidder
406	51-52	Functional Requirements – Solutions	7.3.12	CNAPP shall provide identity and entitlement risk assessment across cloud-native environments	If you are using Kubernetes, is IAM/WIF-based authentication enabled?	Details shall be shared with the successul bidder, the proposed solution should comply with the requirement mentioned in the RFP
407	50-53	Functional Requirements – Solutions	7.3.11 / 7.3.12 / 7.3.13	CSPM/CNAPP/CWPP cover multi-cloud, hybrid-cloud and on-premises environments	The RFP specifies CSPM/CNAPP for public cloud environments. Does the scope also include private or on-premises cloud/data-center environments, such as OpenStack or VMware?	The Solution is required for Public Cloud Ennvironment deployment
408	29-34	Solution & Services Deployment Model	7.2 / 7.2.4	Deployment model and deployment architecture for proposed solutions	Do you need a dedicated tenant/hosting of the application/platform in public cloud ?	Please refer addendum for the revised deployment architecture The security telemetry received and processed by the OEM Cloud/SaaS platform shall be logically segregated and maintained within a dedicated tenant/workspace provisioned
409	50-52	Functional Requirements – Solutions	7.3.11 / 7.3.12	CSPM/CNAPP cloud security, risk assessment, prioritization and remediation	Do you require FinOps capability as part of CSPM/CNAPP platform ?	No Change, Please be guided by the RFP
410	56	Functional Requirements – Services	7.4.4 – Phishing Simulation	Employee awareness, behavioural analysis, user/department risk assessment and identification of high-risk users	Are you looking for a Human Risk Management solution to continuously evaluate and monitor real time risk across all employees based on their actions (for e.g. when a employee is blocked by web gateway trying to access an un-authorized website etc.) apart from risk based on actions during phishing, vishing & smishing simulations?	The requirement is limited to employee awareness, behavioural analysis and risk assessment based on the employee's response to the phishing-simulation activities conducted under the RFP
411		ITDR	1.7	Detect and respond to active threats with high fidelity (low false positives and false negatives).	Pre-Bid Query / Clarification: The Bank has separately specified a comprehensive deception platform for detection of active attacker activity, reconnaissance and lateral movement. We understand that the intent of this clause within ITDR is therefore to complement those controls with focused monitoring of the Bank's most critical identities. Considering that enhanced user-activity monitoring is most relevant for high-risk personnel such as executives, privileged users and other critical users, we request the Bank to kindly clarify whether this requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should provide high-fidelity detection and response for risky or anomalous user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, to identify activities associated with careless, malicious or compromised users.	No Change, Please be guided by the RFP
412		ITDR	1.8	Provide contextual information—who, what, when and how—to inform all stages of the attack chain.	Pre-Bid Query / Clarification: The Bank has already sought attack-lifecycle visibility under the separate deception requirements. For ITDR, we understand that additional value would be derived from detailed user-centric context for the Bank's most critical identities, enabling investigation of risky activity performed by such users. We request the Bank to kindly clarify whether this requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should provide contextual information—who, what, when, where and how—around risky user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, to support investigation and response.	No Change, Please be guided by the RFP
413		ITDR	1.9	Provide deep insights into both the potential and used privilege escalation and lateral movement steps in an attack.	Pre-Bid Query / Clarification: Privilege escalation and lateral-movement visibility is already substantially addressed under the separately specified deception solution, including attacker lifecycle visibility, MITRE ATT&CK mapping, deceptive attack paths and detection of lateral movement. To avoid duplication while retaining complementary investigation capability for high-risk identities, we request the Bank to kindly clarify whether this requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should provide deep insights into activities performed by up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, covering application usage, file and data movement, endpoint activity and other risky behaviours to support investigation of compromised, malicious or negligent user activity.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
414		ITDR	2.9	Detect all types of attack vectors including pre-attack reconnaissance, zero-day attacks, privilege escalation prevention, lateral movement and data theft.	Pre-Bid Query / Clarification: Pre-attack reconnaissance, lateral movement, malware/attack behaviour and attacker lifecycle visibility are already covered under the Bank's separate deception specifications. We understand that the complementary requirement under ITDR should focus on identity/user risk and potential data-loss activity for the Bank's most critical users rather than duplicate the deception control. We request the Bank to kindly clarify whether this requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should detect risky user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, including suspicious application usage, unauthorized access or movement of sensitive information, removable-media activity, web-based transfer, cloud synchronization and other potential data-exfiltration activities.	The Clause is applicable only to idendity related threat vector only. The volumetrics is provided in the RFP and should be complied
415		ITDR	2.10	Detect multiple attacks simultaneously.	Pre-Bid Query / Clarification: We understand the intent is to ensure that the solution is not restricted to investigation of a single event at a time. Since active attacker detection is separately covered by the deception solution, we request that this clause be clarified in terms of concurrent monitoring and investigation of risky activities across the Bank's designated critical-user population: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should be capable of detecting and investigating multiple risky user and data activities simultaneously across up to 100 critical/high-risk users and their monitored endpoints.	No Change, Please be guided by the RFP
416		ITDR	3.2	Provide unified presentation of both source- and target-based telemetry data in a timeline view.	Pre-Bid Query / Clarification: The Bank has separately specified end-to-end attacker visibility and behavioural analysis under the deception solution. For ITDR investigations involving critical identities, a chronological user-activity view would provide complementary evidence of actions performed by the user. We request the Bank to kindly clarify whether the requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should provide a unified chronological timeline of user- and endpoint-based activity telemetry for up to 100 critical/high-risk users identified by the Bank to support investigation of risky or suspicious user activity.	No Change, Please be guided by the RFP
417		ITDR	3.3	Correlate identity-related telemetry from relevant source and target systems to identify and investigate identity compromise, privilege escalation, credential abuse and lateral movement.	Pre-Bid Query / Clarification: Privilege escalation and lateral-movement detection are already addressed through the separately specified deception controls. To provide complementary investigation capability for the Bank's highest-risk identities, we request the Bank to clarify whether this clause may focus on correlation of user, endpoint, application and data activity for the designated critical-user population: Suggested Clarified Wording / Requested Action: The solution shall support correlation of user, endpoint, application and data-activity telemetry for up to 100 critical/high-risk users identified by the Bank to identify and investigate suspicious user behaviour, sensitive-data movement, policy violations and potential data-exfiltration activities.	No Change, Please be guided by the RFP
418		ITDR	3.4	Integrate with compatible endpoint/extended detection solution to capture screen recordings or screenshots during active attacker sessions as advanced forensic evidence.	Pre-Bid Query / Clarification: The Bank has separately specified attacker-session and forensic visibility through the deception platform. Within ITDR, we understand that visual evidence is intended to strengthen investigation of high-risk user activity. We request the Bank to kindly clarify whether the requirement may be read in an outcome-based manner for the designated critical-user population: Suggested Clarified Wording / Requested Action: The Identity Threat Detection Solution should support screenshots, screen capture or equivalent visual evidence of relevant activity for up to 100 critical/high-risk users during suspicious or high-risk user sessions, as part of forensic investigation and evidence collection.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
419		ITDR	3.5	Integrate with compatible network detection solution to support collection of PCAP data for network-level incident visibility.	Pre-Bid Query / Clarification: The requirement for PCAP is network-centric and does not directly relate to identity posture or focused user-activity monitoring. Further, the Bank's separate deception specifications already require high-interaction decoys, recording of attacker activities, traffic/behaviour visibility, forensic investigation and integration with network/security technologies. To avoid duplication of network-level forensic controls across two solution categories, we request the Bank to kindly delete this clause from the ITDR section. Suggested Clarified Wording / Requested Action: Requested action: Delete Clause 3.5 from the ITDR requirements, as equivalent/complementary network and attacker forensic visibility is already sought under the separate Deception requirements.	Please refer addendum for revised clause
420		ITDR	3.6	Push incident data into SIEM/XDR or SOAR technologies via integrations for improved incident management.	Pre-Bid Query / Clarification: We understand that the objective is to ensure relevant ITDR alerts and investigation context are available to the Bank's SOC ecosystem. For the enhanced monitoring of designated critical users, we request the Bank to kindly clarify whether alerts and activity information may be shared through supported integrations or APIs as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should make alerts and relevant incident/activity data for the monitored critical-user population available to SIEM/XDR, SOAR or other supported security platforms through integrations or APIs for improved incident management.	The proposed solution hould be integrated with SIEM/XDR or SOAR technologies for sharing the incident data via supported integrattion or APIs
421		ITDR	3.7	As part of forensic data collection, include detailed attack path information including protocols leveraged during the attack.	Pre-Bid Query / Clarification: Detailed attack-path and attacker-behaviour visibility is already sought under the separate deception specifications, including deceptive attack paths, MITRE ATT&CK mapping and forensic investigation. To avoid overlap while retaining complementary evidence for investigations involving the Bank's critical identities, we request the Bank to kindly clarify whether the requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should, as part of forensic data collection for up to 100 critical/high-risk users, include detailed user-activity information such as applications used, files accessed, data movement, destination channels and other relevant endpoint activity associated with the incident.	Please refer addendum for revised clause
422		ITDR	3.8	Collect user and computer information from Active Directory as part of forensic data gathering to enhance context and assess risk exposure.	Pre-Bid Query / Clarification: We understand that directory information is required to enrich investigations with user and computer context. We request the Bank to clarify that enterprise identity context may be maintained for the overall identity population, while detailed endpoint/user-activity telemetry may be applied to the Bank's designated critical-user population: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should use relevant user and computer identity information to enhance forensic context and risk assessment, and should correlate such context with detailed endpoint/user-activity telemetry for up to 100 critical/high-risk users identified by the Bank.	Please refer addendum for revised clause
423		ITDR	3.9	Detect an adversary's attempt to move laterally toward key assets using as many Windows, Mac or Linux hosts as possible without requiring a persistent agent.	Pre-Bid Query / Clarification: The Bank's separate deception specifications expressly require detection of lateral movement, reconnaissance, credential theft and malicious activity using agentless and/or agent-based deception techniques across the enterprise. The present clause therefore duplicates a capability already being procured under the Deception section. To avoid overlapping scope and duplicate controls, we request the Bank to kindly delete this clause from the ITDR section. Suggested Clarified Wording / Requested Action: Requested action: Delete Clause 3.9 from the ITDR requirements, since lateral-movement detection using deception techniques is already explicitly covered under the separate Deception specifications.	Please refer addendum for revised clause
424		ITDR	3.10	Collect AD user/computer information for forensic context and detect at the earliest point post initial compromise as the attacker first attempts lateral movement and privilege escalation.	Pre-Bid Query / Clarification: Early detection of lateral movement and privilege-escalation activity is substantially covered under the Bank's separate deception requirements. To retain a complementary identity/user-risk objective without duplicating the deception scope, we request the Bank to kindly clarify whether this clause may focus on early detection of risky activity among the designated critical-user population: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should use relevant identity context and detect risky user behaviour at the earliest possible point for up to 100 critical/high-risk users, based on monitored endpoint activities and configured detection policies, enabling investigation and response before such activity results in significant data loss or business impact.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
425		ITDR	3.11	Collect AD user/computer data during forensic gathering while ensuring all deception techniques remain hidden from legitimate users.	Pre-Bid Query / Clarification: The requirement to ensure deception techniques remain hidden from legitimate users is inherently a deception-platform capability. The Bank has already included comprehensive deception requirements covering lures, breadcrumbs, fake credentials, deceptive assets, attacker engagement and techniques designed to remain undetected by attackers. We therefore request the Bank to kindly delete this clause from the ITDR section to avoid duplication. Suggested Clarified Wording / Requested Action: Requested action: Delete Clause 3.11 from the ITDR requirements, as deception techniques and their concealment are already covered under the separate Deception specifications.	Please refer addendum for revised clause
426		Anti Phishing	17.1	Solution should detect at the earliest point in the attack, post initial compromise as the attacker is first attempting to move laterally and escalate privilege.	Pre-Bid Query / Clarification: Since this section is focused on Anti-Phishing, we understand that the objective is to identify suspicious activity following a successful phishing or account-compromise event. Network-level lateral movement and deception capabilities may be addressed by other security controls. We request the Bank to clarify whether this clause may instead focus on early post-compromise user activity visibility for the Bank's most critical users. Suggested Clarified Wording / Requested Action: The solution should support early identification and investigation of suspicious user activities associated with potential account compromise following phishing or other email-originated attacks, with enhanced user activity monitoring for up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles.	Please refer to the relevant Addendum for updated specfications
427		Anti Phishing	17.4	Solution must provide robust supply chain and AI/ML-driven contact chain analysis capabilities to identify and defend against socially engineered, impersonated, or BEC attacks.	Pre-Bid Query / Clarification: As compromise of trusted suppliers and partners is an important source of BEC and phishing risk, we request the Bank to clarify whether the existing supply-chain requirement should explicitly include behavioural analysis of supplier/partner communication patterns to identify attacks originating from compromised trusted accounts. Suggested Clarified Wording / Requested Action: Solution must provide robust supply-chain and AI/ML-driven contact-chain and behavioural analysis capabilities to identify and defend against socially engineered, impersonated or BEC attacks, including threats originating from compromised or impersonated supplier/partner accounts.	Please refer to the relevant Addendum for updated specfications
428		Anti Phishing	18	Solution must proactively analyze suspicious URLs using dynamic/behavioral analysis to prevent the spread of malware and other threats.	Pre-Bid Query / Clarification: The RFP separately addresses URL analysis and post-delivery remediation. We request clarification whether these requirements are intended to provide continuous protection throughout the email threat lifecycle, including pre-delivery analysis, click-time URL protection and post-delivery detection/remediation. Suggested Clarified Wording / Requested Action: Solution must provide continuous protection across the email threat lifecycle, including pre-delivery threat detection, real-time/click-time inspection of suspicious URLs, and post-delivery detection and automated remediation of threats that are subsequently determined to be malicious.	Please refer to the relevant Addendum for updated specfications
429		Anti Phishing	19.7	Solution must be able to offer a comprehensive portal that allows users to access information and metadata on events/incidents, facilitating network threat forensics for thorough investigation and analysis of potential security breaches or incidents.	Pre-Bid Query / Clarification: To strengthen investigation of phishing-led incidents involving executives and other critical users, we request clarification whether the existing forensic portal requirement may also include contextual user and endpoint activity for a limited population of Bank-identified critical/high-risk users. Suggested Clarified Wording / Requested Action: Solution must offer a comprehensive investigation portal providing information and metadata on events/incidents for forensic analysis. For up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, the portal should additionally provide contextual user and endpoint activity, including relevant application, file and user-action details, to support investigation of potential phishing-led compromise.	Please refer to the relevant Addendum for updated specfications
430		Anti Phishing	19.9	Solution must empower security operations and incident responders to automate the identification, remediation, and sharing of phishing threats, streamlining the process of detecting, addressing, and disseminating information about potential phishing attacks for improved response and mitigation.	Pre-Bid Query / Clarification: To improve SOC investigation efficiency, we request clarification whether the existing phishing identification and remediation requirement should include centralized attack context showing why a message was identified as malicious, the users targeted, associated threat indicators and remediation status. Suggested Clarified Wording / Requested Action: Solution must empower security operations and incident responders to automate identification, investigation, remediation and sharing of phishing threats, and should provide centralized contextual visibility into the users targeted, associated threat indicators, detection rationale, attack characteristics and remediation actions.	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
431		Anti Phishing	19.1	Solution must provide incident responders with real-time analytics and visibility into email-based attacks targeting the organization.	Pre-Bid Query / Clarification: Email-based attacks against executives and privileged users may require additional context after delivery to determine whether a targeted user has subsequently performed suspicious activity. We request the Bank to clarify whether real-time investigation visibility may include relevant user activity context for up to 100 Bank-identified critical/high-risk users. Suggested Clarified Wording / Requested Action: Solution must provide incident responders with real-time analytics and visibility into email-based attacks targeting the organization. For up to 100 Bank-identified critical/high-risk users, the solution should additionally provide contextual visibility into suspicious user activities associated with potential phishing or account compromise, including relevant user, endpoint, application and file activity.	Please refer to the relevant Addendum for updated specfications
432		Anti Phishing	19.23	Solution must have simplicity of evaluation and additional visibility into internal traffic and other communication channels can reduce risk, and baseline user activity to detect suspicious behavior.	Pre-Bid Query / Clarification: The existing clause already seeks baselining of user activity to detect suspicious behaviour. We request the Bank to clarify the intended depth and scope of this capability and whether enhanced monitoring may be applied to a focused population of up to 100 Bank-identified critical/high-risk users, where deeper visibility provides the greatest security value. Suggested Clarified Wording / Requested Action: Solution must provide additional visibility into relevant internal activity and communication channels to reduce risk and baseline user activity to detect suspicious behaviour. Enhanced user and data activity monitoring should be provided for up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, with configurable detection policies for suspicious, anomalous or policy-violating activities.	Please refer to the relevant Addendum for updated specfications
433		Anti Phishing	19.7	Solution must provide protection against harassment mail and mitigate the risks associated with emails from unknown senders specifically for executives or VIPs, safeguarding them from potential threats and ensuring their email communication remains secure.	Pre-Bid Query / Clarification: Since this clause already provides enhanced protection for executives/VIPs, we request the Bank to clarify whether such enhanced protection should extend beyond receipt of suspicious email to investigation of risky user and data activities that may occur following phishing or account compromise, for a limited set of the Bank's most critical users. Suggested Clarified Wording / Requested Action: Solution must provide protection against harassment mail and mitigate risks associated with emails from unknown senders specifically for executives or VIPs. For up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, the solution should additionally provide enhanced visibility into risky user and data activities following suspected phishing or account compromise, including relevant file movement, web/upload activity, removable-media activity and other supported data-transfer channels.	Please refer to the relevant Addendum for updated specfications
434		Cloud	1	OEM shall ensure compliance of the complete proposed solution & platform with RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and all applicable regulations throughout the contract period.	Pre-Bid Query / Clarification: We request the Bank to clarify that the OEM is required to maintain applicable security, privacy and regulatory controls relevant to the services provided and furnish available compliance/assurance documentation, while the overall regulatory compliance obligation of the Bank remains subject to the Bank's deployment, configuration and usage of the service. Suggested Clarified Wording / Requested Action: OEM shall maintain security, privacy and compliance controls applicable to the proposed hosted service and shall provide available independent assurance reports, certifications and relevant compliance documentation to support the Bank's obligations under applicable RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and other applicable regulatory requirements.	Please refer addendum for revised clause
435		Cloud	2	The Service uptime agreement for the proposed solution on cloud should have monthly uptime commitments and have transparent monthly credit calculations in case of uptime not being met for any services.	Pre-Bid Query / Clarification: We understand that published/contracted OEM hosted-service SLA commitments and corresponding service-credit methodology shall meet this requirement. Kindly confirm. Suggested Clarified Wording / Requested Action: Retain clause, with clarification that the applicable OEM hosted-service SLA and service-credit schedule will govern the commitment.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
436		Cloud	3	Solution provider should provide the design and process for data deletion in the scope of an independent audit and that the operational effectiveness of these controls is tested. The report for the same should be submitted to bank as and when asked by bank.	Pre-Bid Query / Clarification: For a globally operated hosted security service, control effectiveness is generally evidenced through independent assurance reports such as SOC 2 Type II and documented data-retention/deletion controls. We request the Bank to permit such independent assurance documentation instead of requiring a separate bespoke data-deletion audit report. Suggested Clarified Wording / Requested Action: Solution provider shall maintain documented secure data-retention and deletion controls. Compliance may be demonstrated through applicable independent third-party assurance reports/certifications (such as SOC 2 Type II or equivalent) and documented data-retention/deletion policies made available subject to OEM confidentiality requirements.	Please refer addendum for the revised clause
437		Cloud	4	Independent audit for testing effectiveness of secure data removal, such that data is rendered permanently inaccessible. (Including any backup or distributed online media).	Pre-Bid Query / Clarification: We request the Bank to accept independently audited secure deletion and media-management controls, together with documented retention/deletion periods, rather than requiring a customer-specific audit of all backup and distributed media. Suggested Clarified Wording / Requested Action: The OEM shall maintain secure data deletion, media handling and backup-retention controls designed to render customer data inaccessible in accordance with documented retention schedules. Effectiveness may be evidenced through independent assurance reports such as SOC 2 Type II/ISO 27001 or equivalent and relevant OEM security/privacy documentation.	Please refer addendum for the revised clause
438		Cloud	5	Bank shall have an option to implement 'Bring Your Own Key' as and when required.	Pre-Bid Query / Clarification: The proposed service protects data at rest and in transit using strong encryption; however, customer-managed infrastructure encryption keys are not a standard capability of the hosted anti phishing service. We request deletion of the BYOK requirement, or acceptance of OEM-managed enterprise-grade encryption and key-management controls. Suggested Clarified Wording / Requested Action: Requested Action: Delete the BYOK requirement. Alternatively: 'Data processed/stored by the hosted service shall be protected using industry-standard encryption in transit and at rest, with secure OEM-managed key-management controls subject to independent security assurance.'	Please refer addendum for the revised clause
439		Cloud	6	Web Application Firewall shall be implemented on the cloud for Web based applications. WAF application signature should be updated and reviewed regularly. The Report shall be submitted to bank on a periodic interval.	Pre-Bid Query / Clarification: Since the proposed platform is an OEM-managed hosted security service, underlying WAF technology, signatures and configurations form part of the OEM's internal security architecture and may not be exposed as customer-specific reports. We request the Bank to accept periodic VAPT/penetration-test assurance or equivalent independent security assessment evidence covering the hosted application instead of WAF signature reports. Suggested Clarified Wording / Requested Action: The hosted web application/platform shall be protected through appropriate application-security controls. The OEM shall conduct periodic vulnerability assessment and penetration testing/security assessments and, subject to confidentiality restrictions, provide an executive summary/attestation or applicable independent assurance evidence to the Bank on request. Customer-specific WAF signature reports shall not be mandatory.	Please refer addendum for revised clause
440		Cloud	7	The systems in cloud infrastructure should be periodically updated with the latest anti-malware signatures, the bidder shall submit the periodic report on the same with bank.	Pre-Bid Query / Clarification: For an OEM-managed hosted security service, infrastructure anti-malware/endpoint controls are centrally managed and independently audited. We request the Bank to accept OEM security assurance and vulnerability/malware-control attestations rather than periodic host-level signature reports. Suggested Clarified Wording / Requested Action: The OEM shall maintain appropriate malware protection, vulnerability management, patching and security monitoring controls for the hosted infrastructure. Compliance may be evidenced through independent assurance reports/certifications and applicable security-control attestations instead of customer-specific anti-malware signature update reports.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
441		Cloud	8	Data Loss Governance and risk management framework shall be defined by bidder for workload on the cloud and same shall be shared with bank on periodic basis. Data loss prevention controls should be implemented to secure the data in the cloud environment from unauthorized or inadvertent exfiltration.	Pre-Bid Query / Clarification: We request clarification that the requirement is intended to ensure protection against unauthorized/inadvertent data exfiltration through the proposed service and appropriate security controls for hosted customer data, rather than requiring disclosure of the OEM's internal cloud governance framework. Suggested Clarified Wording / Requested Action: The proposed solution shall provide configurable controls to identify and prevent unauthorized or inadvertent transmission/exfiltration of sensitive information through any channels. The OEM shall maintain appropriate access control, encryption and data-protection controls for customer data processed within the hosted service and provide applicable assurance documentation on request.	Please refer addendum for revised clause
442		Cloud	9	Log generation, storage and review process should be certified by CERT IN empaneled auditor, report for the same shall be submitted by bidder as and when required by bank.	Pre-Bid Query / Clarification: For global SaaS/POD services, security logging and monitoring controls are typically independently audited under recognized assurance frameworks. We request the Bank to accept SOC 2 Type II/ISO 27001 or equivalent independent assurance in lieu of a mandatory CERT-In-empanelled audit of the OEM's internal log-generation/storage/review process. Suggested Clarified Wording / Requested Action: The OEM shall maintain documented security logging, monitoring, retention and review controls. Effectiveness shall be evidenced through applicable independent third-party assurance reports/certifications such as SOC 2 Type II, ISO 27001 or equivalent. CERT-In-empanelled audit may be required only for bidder-managed components deployed specifically within the Bank environment, where applicable.	Please refer addendum for the revised clause
443		Cloud	10	IT Act 2000 & its amendments, and other Acts/Regulatory guidelines.	Pre-Bid Query / Clarification: Kindly clarify that the OEM must comply with legal/regulatory requirements applicable to it as the provider of the proposed hosted service and provide reasonable documentation to support the Bank's compliance obligations. Suggested Clarified Wording / Requested Action: OEM shall comply with applicable legal and regulatory obligations relevant to its provision of the proposed service and shall provide available security/privacy/compliance documentation reasonably required to support the Bank's applicable obligations.	Please refer addendum for the revised clause
444		Cloud	11	CERT IN Empaneled auditor report's is required for the following:	Pre-Bid Query / Clarification: We request the Bank to permit internationally recognized independent assurance reports/certifications for OEM-managed hosted services. CERT-In empanelled audit reports may remain applicable to India-specific bidder-managed/on-premises components where such audit is feasible and required. Suggested Clarified Wording / Requested Action: For OEM-managed hosted/SaaS services, independent assurance reports/certifications such as SOC 2 Type II, ISO 27001 or equivalent shall be accepted. CERT-In empanelled audit reports shall be applicable only to components/services for which such India-specific audit is contractually and technically feasible.	Please refer addendum for the revised clause
445		Cloud	12	The application and DB is/will be hosted separately on a dedicated infrastructure (physical/logical) for PSB. Evidence of dedicated infrastructure (physical/logical) for PSB should be submitted.	Pre-Bid Query / Clarification: The proposed platform is an OEM-managed hosted security service designed with logical access controls and customer data isolation. Requiring dedicated physical application/database infrastructure would restrict standard SaaS/POD architectures without necessarily improving the security outcome. We request acceptance of secure logical tenant/customer isolation supported by independent assurance evidence. Suggested Clarified Wording / Requested Action: The proposed hosted service shall provide secure logical segregation/isolation of Bank data and administrative access from other customers through appropriate access-control and tenant-isolation mechanisms. Dedicated physical application/database infrastructure shall not be mandatory where equivalent logical isolation is implemented and independently assured.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
446		Cloud	13	Feasibility to audit/review IT controls of the third party or obtaining independent review report for the same from CERT-In empaneled security consultant, to ensure it meets Bank's information security requirement.	Pre-Bid Query / Clarification: We request that the Bank permit review of current independent assurance reports/certifications as the primary mechanism for reviewing OEM IT controls. Any direct audit should remain subject to the OEM's standard contractual audit provisions, confidentiality, security, scope and advance-notice requirements. Suggested Clarified Wording / Requested Action: The Bank may review applicable independent third-party assurance reports/certifications covering the hosted service. Where additional audit is required, such audit shall be subject to mutually agreed scope, confidentiality/security restrictions, reasonable advance notice and the OEM's standard contractual audit provisions. A CERT-In empanelled consultant may review evidence made available under these conditions.	Please refer addendum for revised clause
447	117	10.2	Eligibility Criteria-Clause-22	The proposed OEM solution should have been implemented in at least one verifiable client in India. Credential is to be submitted for the following solutions: a. CNAPP b. CWPP c. CTEM	CTEM is a new framework and customers are still in evaluation/ Implementation phase. Suggested change Client in India or Global BFSI The proposed OEM solution should have been implemented in verifiable client in India or Global. Credential is to be submitted for each of the following solutions: 1. CNAPP 2. CWPP 3. CTEM	No Change, Please be guided by the RFP
448	120	10.2	Eligibility Criteria-Clause-23	The proposed OEM services should have been implemented in at least one (1) PSU/ PSE/ Government Organizations / BFSI in India. Credential is to be submitted for the following services: 1. Breach Attack & Simulation 2. Continuous Automated Red Teaming 3. Attack surface management 4. Phishing simulation 5. Anti-phishing services 6. Dark web monitoring 7. Brand protection & monitoring 8. Threat Intelligence feed 9. Threat Hunting services	As the offsite services are specified under the functional compliance requirements and are expected to be provided by the bidder, the corresponding eligibility criteria should be assessed at the bidder level. Suggested Changes: The proposed bidder services (below mentioned to the services) should have been implemented by the bidder in in at least one verifiable client in India.	No Change, Please be guided by the RFP
449	86	16	Technical Specs-Anti Phishing-	Solution must be able to seamlessly integrate with On-Prem Mail Gateways via Mail Transfer Agent (MTA) forwarding	Anti-Phishing is asked as a Managed service however MTA is a componentfor onprim SEG gateway Suggested Change: Solution must be able to seamlessly integrate with On-Prem Mail Gateways via API integration	Please refer to the relevant Addendum for updated specfications
450	87	18.2	Technical Specs-Anti Phishing-	Solution must provide DoS protection and directory harvest attack protection to ensure the availability of email services	DOS Protection Is Typically the Responsibility of the hardware based Email Infrastructure or Secure Email Gateway or Firewall or dedicated DDOS protection Hence this clause should not fall under Anti-Phishing services Also, this feature Suggested Change: Remove this clause	Please refer to the relevant Addendum for updated specfications
451	87	19.2	Technical Specs-Anti Phishing	Solution must be able to display HTML banners on email clients, automatically switching to plain text format if HTML is not supported, while also providing multilingual support based on the organization's language preferences. HTML banner content can be edited or customized by organization	The requirement appears to prescribe a specific notification mechanism (HTML banner insertion) rather than the intended security outcome of user awareness and phishing risk notification. Modern anti-phishing solutions may provide user alerts through native email client warnings, subject tagging, security indicators, API-based notifications, or other mechanisms without relying on HTML banner injection. Suggested Change: Remove the clause	Please refer to the relevant Addendum for updated specfications
452	87	19.4	Technical Specs-Anti Phishing	Solution must offer multiple disposition options, including attachment stripping, delivery of notices to senders, and quarantine of the whole email	Delivery of notice is platform specific feature Suggested Change Solution must offer multiple disposition options, including attachment stripping, and quarantine of the whole email	Please refer to the relevant Addendum for updated specfications
453	87	19.5	Technical Specs-Anti Phishing	Solution must provide a "Safe Preview" capability for administrators to view detailed information of quarantined messages and decide necessary actions	Safe Preview is a broad term, it should relate to anti-phishing Suggested Change Solution must provide a "Safe Preview of links" capability for administrators to view detailed information of quarantined messages and decide necessary actions	Please refer to the relevant Addendum for updated specfications
454	88	19.8	Technical Specs-Anti Phishing-	As part of the forensic collection, should include the capture of PowerShell history	The requirement appears to mandate a specific forensic artefact (PowerShell history) rather than the intended security objective of investigating PowerShell-based activity. Suggested Change As part of the forensic collection, should include the capture of PowerShell history or equivalent forensic mechanism	Please refer to the relevant Addendum for updated specfications
455	88	19.17	Technical Specs-Anti Phishing-	Solution must provide detailed reporting covering system usage and other areas including global message summary, spam, virus and other rule actions to save administrator time and effort in the collection of data for status reports. Reports can be emailed (HTML), printed, or downloaded in CSV format for use with third party tools	Suggested Changes: Solution must provide detailed reporting covering system usage and other areas including global message summary, spam, virus and other rule actions to save administrator time and effort in the collection of data for status reports. Reports can be emailed (HTML), printed, or downloaded in CSV or PDF format for use with third party tools	Please refer to the relevant Addendum for updated specfications
456	88	19.18	Technical Specs-Anti Phishing-	Solution must have capability for administrators to view reports containing detailed statistics covering emails processed, rejected emails, SMTP transactions, and communication flows	The requirement mandates visibility into SMTP transactions and communication flow analytics, which are traditionally functions of MTA,and may not have direct access in API-based or cloud-native anti-phishing solutions. Suggested Change Solution must have capability for administrators to view reports containing detailed statistics covering emails processed, rejected emails.	Please refer to the relevant Addendum for updated specfications
457	89	19.37	Technical Specs-Anti Phishing-	Solution must support message classification management, including separate classifiers for spam, impersonation, bulk, phishing, adult, and malware messages, with the ability to set score thresholds per category.	The requirement mandates a specific detection architecture based on separate classifiers and per-category scoring thresholds. Modern email security and anti-phishing solutions increasingly leverage AI/ML models, behavioural analytics, graph intelligence, and composite risk engines that may not expose individual classifiers Suggested Change Solution must support message classification management, including separate classifiers for spam, impersonation, bulk, phishing and malware messages, with the ability to set score thresholds per category.	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
458	89	19.41	Technical Specs-Anti Phishing	Solution must provide granular administrative controls to allow role-based access to each module and quarantine folder.	Modern cloud-native anti-phishing solutions implement administrative segregation through configurable RBAC, delegated administration, role groups, and permission-based access models, which may not necessarily expose permissions at the individual module or quarantine-folder level Suggested Change Solution must provide granular administrative controls to allow role-based access	Please refer to the relevant Addendum for updated specfications
459	89	19.43	Technical Specs-Anti Phishing	Solution must support complicated mail routing requirements, including group-based routing based on user groups	The requirement appears to address email infrastructure and mail-flow routing capabilities rather than core anti-phishing or email threat protection functionality. Complex mail routing, transport rules, and group-based routing are typically implemented within the email platform Suggested Change Remove this clause, its not applicable	Please refer to the relevant Addendum for updated specfications
460	89	19.5 0	Technical Specs-Anti Phishing	solution must support a range of routing behaviors and actions for different scenarios, allowing administrators to customize email handling based on specific needs and requirements.	The requirement is broad and appears to focus on email routing and mail-flow management capabilities, which are typically functions of the email infrastructure (Microsoft Exchange, Exchange Online Suggested Change Remove this clause, its not applicable	Please refer to the relevant Addendum for updated specfications
461	90	19.51	Technical Specs-Anti Phishing	Solution must support for in outbound or inbound email including footer management Inserting one or more legal or compliance footers (e.g. disclaimer) Multi-language support Apply different filters based on email attributes or active directory attributes, Insert dynamic content to footer such as date, when to apply the footer in the message routing hops, Selectively apply based on policy / attribute or not apply if the email is s/mime encrypted or digitally signed, etc Apply signatures and disclaimers based on AD user groups	Footer management is vendor specific feature Suggested Change Remove the clause	Please refer to the relevant Addendum for updated specfications
462	90	19.5 3	Technical Specs-Anti Phishing	Solution must allow end-users to receive customized email notifications based on domain name.	The clause prescribes a specific notification customization method (domain-based) that may not be supported by all modern cloud-native Anti-Phishing solution Suggested Change: Solution must allow end-users to receive customized email notifications based alerts, and awareness messages based on organizational policies	Please refer to the relevant Addendum for updated specfications
463	90	19.5 7	Technical Specs-Anti Phishing	Solution must provide administrators with capabilities for email queue management	This feature is excahnge or onprim gateway specific. Suggested Change Remove the clause	Please refer to the relevant Addendum for updated specfications
464	90	19.5 9	Technical Specs-Anti Phishing	Solution must support alerting the security team on all policies, quarantine folders, and queue thresholds	The clause is a gateway-specific alerting model based on quarantine folders and queue thresholds. Modern cloud-native email security solutions may not utilise traditional mail queues while still providing comprehensive alerting for security incidents, policy actions, quarantine events, and operational status Suggested Change Solution must support alerting the security team on all policies, quarantine folders, and queue thresholds or equivalent alerting mechanism	Please refer to the relevant Addendum for updated specfications
465	90	19.6 2	Technical Specs-Anti Phishing	Solution must provide application and message routing troubleshooting tools with a message-tracing capability to facilitate help desk work	Message routing trobleshooting & message-tracing capabilities are part of exchange provider. Suggested Change Remove the clause	Please refer to the relevant Addendum for updated specfications
466	53	7.3.14	Paragraph 2 of the CTEM scope	The Bidder shall leverage all the required services and technologies to provide an integrated, unified 'Risk Dashboard' that operationalizes the 5 stages of the CTEM framework (Scoping, Discovery, Prioritization, Validation, and Mobilization).	The scored compliance sheet at Appendix 1A contains no line item for the Scoping stage and no line item for CTEM program stages, which is the capability that distinguishes stages like Prioritization in the CTEM framework from conventional vulnerability ranking methodology. Request the Bank to confirm whether the unified Risk Dashboard must be delivered by a single CTEM OEM product or may aggregate outputs from the Bank's other procured solutions, and request that Appendix 1A be amended to score each of the five stages named in this clause in a unified scoring mechanism. If this is not done then purpose of CTEM will be defeated and bank will again be stuck with siloed tool approach for Threat and risk scoring	Please refer addendum for revised clause
467	53	7.3.14.1	Sub-clause 2	The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Request the Bank state the authentication protocol its MFA platform exposes, whether SAML 2.0, OpenID Connect or RADIUS, and confirm that federation to the Bank's identity provider through a standard protocol satisfies this requirement without the CTEM OEM being required to integrate with a named MFA product.	Please refer addendum for revised clause
468	53	7.3.14.1	Sub-clause 3	The solution shall support creation and management of CTEM scopes based on business units, applications, assets, asset groups, environments, technologies, locations, business criticality and other Bank-defined criteria.	Scoping is the first stage of the CTEM framework and this requirement carries no corresponding line item or marks in the Appendix 1A compliance sheet. This is more from a Vulnerability Scanning perspective scoping. For CTEM Scoping comprises of multiple Asset inventories and other mechansims and it involved External and INternal assets of the organization. Request the Bank to add a scored specification for scope creation and management to Appendix 1A, and state which scope dimensions are mandatory at go-live so that bidders can size the onboarding effort.	No Change, Please be guided by the RFP
469	53	7.3.14.1	Sub-clause 4	The solution shall support identification of business-critical assets and attack surfaces within defined CTEM scopes.	This requirement carries no corresponding line item in Appendix 1A. Request the Bank add a scored specification for it, and confirm whether the Bank will supply an asset criticality register or CMDB extract from which business criticality can be derived, or whether the CTEM solution is expected to determine criticality independently. Also, the Attack Surface is asked as a separate service.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
470	53	7.3.14.1	Sub-clause 5	The solution shall support association of business criticality and relevant business context with assets and exposures for risk assessment.	Request the Bank identify the authoritative source of business context it will make available, whether a CMDB, an application register or confidentiality, integrity and availability ratings, the format in which it will be provided, and the update frequency, since the accuracy of risk-based prioritisation depends entirely on this input.	No Change, Please be guided by the RFP
471	53	7.3.14.1	Sub-clause 6	The solution shall support re-validation of exposures after remediation or security-control changes.	Re-validation closes the CTEM loop and this requirement carries no corresponding line item in Appendix 1A. Request the Bank add a scored specification for it, and state the expected re-validation service level following a remediation record being closed.	No Change, Please be guided by the RFP
472	53	7.3.14.1	Sub-clause 7	The solution shall maintain historical records of validation activities, validation results and exposure-status changes.	This requirement carries no corresponding line item in Appendix 1A. Request the Bank add a scored specification for it, and state the retention period required for validation records, since validation evidence is normally the artefact presented to regulators and auditors.	No Change, Please be guided by the RFP
473	53	7.3.14.1	Sub-clause 8	The solution shall maintain linkage between the identified exposure, affected asset, remediation action and validation result throughout the exposure-management lifecycle.	This is the core CTEM data model and it carries no corresponding line item in Appendix 1A. Request the Bank add a scored specification for exposure lifecycle linkage so that the compliance sheet tests the capability the scope of work requires.	No Change, Please be guided by the RFP
474	53	7.3.14.1	Sub-clause 10	The solution shall provide attack-path visualisation showing relationships between affected assets, security weaknesses and potential paths to critical assets based on available integrated data.	Attack-path visualisation is the capability that distinguishes Continuous Threat Exposure Management from conventional vulnerability management, and it is the single most important requirement in this section. It carries no line item and no marks in the 690 mark Appendix 1A compliance sheet that determines the 85 percent eligibility gate. Request the Bank add a scored specification for attack-path discovery, visualisation and choke-point identification, with marks proportionate to its importance.	No Change, Please be guided by the RFP
475	54	7.3.14.1	Sub-clause 14	The solution shall provide trend analysis to measure changes in overall exposure, critical exposures, validated exposures and remediation effectiveness over time.	This requirement carries no corresponding line item in Appendix 1A. Request the Bank add a scored specification for exposure trend analysis, and state the reporting periods over which trends must be presented.	No Change, Please be guided by the RFP
476	54	7.3.14.2	Key deliverable 6	Periodic Exposure Review & Risk Trend Report.	Request the Bank state the required frequency of the periodic exposure review and risk trend report, the audience, and whether the review is a document submission or a facilitated session with the Bank, since this determines the analyst effort to be priced.	No Change, Please be guided by the RFP
477	31	7.2.1	Master Deployment Matrix, row 14 (CTEM)	Continuous Threat Exposure Management (CTEM). Deployment Mode: Cloud (SaaS) + Hybrid. HA Requirement: Cloud (SaaS): Deployment aligned with the SLA, RTO & RPO (Refer Section 13). Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Management Console: Deployed at both Primary and Secondary sites.	This clause mandates Bank-hosted CTEM components in N plus N Active-Active configuration at both DC and DR, while Appendix 1A CTEM item 38 requires the solution to be deployed agentlessly without sensors or agents. An agentless cloud platform has no Bank-hosted component to deploy in N plus N Active-Active and no management console to install at either site. Request the Bank confirm that for CTEM the high availability obligation applies only to the cloud platform's own resiliency in accordance with the applicable SLA, RTO and RPO, and that no Bank-hosted CTEM component, virtual machine, appliance or management console is required.	Please refer Addendum for Revised Clause
478	31	7.2.1	Note below the Master Deployment Matrix	For solutions deployed in Cloud (SaaS) + Hybrid mode, any agents, sensors, collectors, connectors, brokers, aggregators, gateways, enforcement components or other components required to be deployed within the Bank's infrastructure shall be provided, deployed, configured, maintained and supported by the Bidder/OEM as part of the proposed solution and shall be included in the quoted cost.	Where a Bank-side component is required the bidder must price it, but the RFP does not state the number of endpoints, servers or network segments on which such components would be deployed for each solution. The functional requirememt set in the RFP are not mapped and specified in line with the specifications in Appendix 1A. Request the Bank state, per solution, the expected count of agents, sensors, collectors and gateways to be deployed within the Bank's infrastructure, so that the no separate cost obligation can be priced rather than assumed.	No Change, Please be guided by the RFP
479	33	7.2.3	Deployment Model Definition, clause 2, final bullet	Partial HA deployment of any critical Bank-hosted component for which HA is mandated shall not be accepted.	Request the Bank confirm that where a solution is delivered wholly as SaaS with no Bank-hosted component, this clause is not applicable and the bid will not be treated as non-responsive on that ground.	The HA requirement shall apply wherever HA is specified/mandated under the RFP for an on-premise/Bank-hosted component. **Fully On-Premise:** HA shall be implemented for all the solutions/components for which HA is mandated under the RFP as per the deployment requirement mandated in the RFP. **Fully Cloud/SaaS**: The cloud/SaaS service shall comply with the applicable availability, resilience and SLA requirements of the RFP. **Hybrid- Component On-Premise and Cloud:** HA, as per deployment requirement, shall be implemented for all components hosted within the Bank's DC/DR for which HA is mandated under the RFP. Cloud/SaaS components shall comply with the applicable cloud service availability, resilience and SLA requirements. Partial HA deployment shall not be accepted for any Bank-hosted component for which HA is mandated under the RFP.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
480	Appendix 3	Appendix 3	Cloud BOQ and Virtual to Physical mapping, CTEM rows	Continuous Threat Exposure Management (CTEM), environments DC-Primary, DC-HA, DR-Primary, DR-HA and Non-production, with VM count, vCores per VM, RAM per VM, HDD per VM, primary, object and long term storage capacity and per-VM operating system, application server, web server and database licensing.	Request the Bank confirm that these rows may be marked not applicable where the CTEM solution is delivered as SaaS with no Bank-hosted component, and that no reduction in marks and no finding of non-responsiveness will follow from doing so.	Bidder based on their architecture to propose the component. However, bank specific requirement for deployment, HA and SLAs is to be complied In case of Cloud (SaaS): Deployment aligned with the uptime SLA (Refer Section 13).
481	256	Annexure 21	Volumetrics item 1, Non-Production Environment	For VM-based solutions, the non-production environment shall be sized at a minimum of 10% of the Production (DC) environment unless otherwise specified in the RFP.	Request the Bank confirm that this requirement does not apply to solutions delivered as SaaS with no Bank-hosted virtual machines, and state whether a separate non-production tenant is required for such solutions and whether it is to be quoted.	Please refer addendum for revised clause
482	Appendix 1A, page 18	Appendix 1A - CTEM	CTEM item 1	The solution should collect intelligence from multiple languages and relevant regional sources, with support for multilingual threat intelligence processing and analysis.	Multilingual intelligence collection is a Digital Risk Protection attribute and is already scored in the Threat Intelligence Feed sheet at Appendix 1C item 1, which requires collection in more than 20 languages. The functional requirememt set in the RFP are not in sync with required technical compliance asked in Appendix 1A. Request the Bank delete this item from the CTEM sheet, or move this to Threat intel Feed Appendix 1C section.	Please refer addendum for revised clause
483	Appendix 1A, page 18	Appendix 1A - CTEM	CTEM item 2	The solution should support translation or interpretation of collected intelligence into English	Translation of collected intelligence into English is a Digital Risk Protection portal function and has no bearing on exposure management. The functional requirememt set in the RFP are not in sync with required technical compliance asked in Appendix 1A. Request the Bank delete this item from the CTEM sheet or confirm that it is retained only in the Dark Web Monitoring and Threat Intelligence Feed sheets.	Please refer addendum for revised clause
484	Appendix 1A, page 18	Appendix 1A - CTEM	CTEM item 6	The solution should enrich intelligence results and filter by author, severity, source, date, asset association, and other criteria	Filtering by asset association, severity, source and date is consistent with exposure management, but filtering by intelligence author is a Digital Risk Protection portal construct. The functional requirememt set in the RFP are not in sync with required technical compliance asked in Appendix 1A. Request the Bank confirm that filtering by author is not mandatory, or split the item so that the exposure-relevant filters are scored and the author filter is not.	No Change, Please be guided by the RFP
485	Appendix 1A, page 18	Appendix 1A - CTEM	CTEM item 7	Each intelligence item should include metadata such as date, author, source, and pre-classification of raw data	Per-item metadata including author and pre-classification of raw data describes the data model of a threat intelligence portal rather than an exposure record. Request the Bank confirm whether this item is intended to apply to exposure findings or only to threat intelligence items, and if the latter, relocate it to the Threat Intelligence Feed sheet.	Please refer addendum for revised clause
486	Appendix 1A, page 18	Appendix 1A - CTEM	CTEM item 10	Analysts should perform threat hunting activities to find findings outside of the platform	This item requires human analysts to conduct threat hunting outside the platform. Appendix 1A permits only S, defined as standard product functionality available out of the box or achievable through parametrisation or rules configuration, and C, defined as minor customization, and instruction 4 states that any other response is treated as N with the bid liable for rejection. A product OEM cannot truthfully record either response against a human analyst service. The functional requirememt set in the RFP are not in sync with required technical compliance asked in Appendix 1A. Request the Bank relocate this item to Appendix 1C, or add a response category for contractual service commitments, or confirm in writing that a binding service commitment may be recorded as S.	Please refer addendum for revised clause
487	Appendix 1A, page 18	Appendix 1A - CTEM	CTEM item 11	The solution/service should generate investigation reports for designated VIPs or other high-risk identities/assets, providing an overview of identified digital exposure and associated risk.	Investigation reports for designated VIPs are an analyst deliverable rather than a product feature, and executive exposure monitoring is already scored in the Dark Web Monitoring sheet. Request the Bank relocate this item to Appendix 1C, and state the number of designated VIP identities in scope so that the analyst effort can be priced.	No Change, Please be guided by the RFP
488	Appendix 1A, page 18	Appendix 1A - CTEM	CTEM item 12	The solution should provide general and industry-related cyber intelligence reports on threat landscape trends, at least twice a month	A publication schedule of at least twice a month is a service commitment, not product functionality, and general and industry threat landscape reporting is already scored in the Threat Intelligence Feed sheet. Request the Bank relocate this item to Appendix 1C or delete it as duplicative.	Please refer addendum for revised clause
489	Appendix 1A, page 18	Appendix 1A - CTEM	CTEM item 13	The solution should be able to commission ad-hoc research reports on demand	Commissioned ad-hoc research is a bespoke analyst service and cannot be scored as standard product functionality. Request the Bank relocate this item to Appendix 1C and state the number of ad-hoc research reports included per contract year, so that the commitment can be priced rather than left open-ended.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
490	Appendix 1A, page 18	Appendix 1A - CTEM	CTEM item 16	The solution should support IOC reputation queries via direct API	These are part of Threat intelligence feed capabilities. The CTEM functional requirememt set in the RFP are not in sync with required technical compliance asked in Appendix 1A. Request the Bank to move this clause to Threat Intel Feed section.	No Change, Please be guided by the RFP
491	Appendix 1A, page 18	Appendix 1A - CTEM	CTEM item 19	The solution should detect compromised credentials for employees and VIPs, exposed payment card information, and aggregate data from known breach databases in real time	These are part of Dark Web Monitroing capabilities. The CTEM functional requirememt set in the RFP are not in sync with required technical compliance asked in Appendix 1A. Request the Bank to move this clause to Dark Web monitoring services section.	Please refer addendum for revised clause
492	Appendix 1A, page 18	Appendix 1A - CTEM	CTEM item 21	The solution should support threat actor interaction via vendor analysts (e.g., engaging via dark web avatars) to gather additional intelligence	Engagement with threat actors through dark web avatars is a human intelligence operation conducted by a small number of Digital Risk Protection providers. As a scored functional specification in a CTEM product sheet it is a restrictive requirement that narrows the field on a basis unrelated to exposure management outcomes, and it cannot be answered S by any product OEM. The CTEM functional requirememt set in the RFP are not in sync with required technical compliance asked in Appendix 1A. Request the Bank to move this clause to Threat Intel Feed section." Request the Bank delete this item from the CTEM sheet, and move it to Threat intel feed section alongwith Threat itel platform capabilities	Please refer addendum for revised clause
493	Appendix 1A, page 18	Appendix 1A - CTEM	CTEM item 23	The solution should support reporting of confirmed malicious or phishing assets to relevant external platforms and authorities, where such reporting is supported and authorized.	Reporting confirmed malicious or phishing assets to external platforms and authorities is a takedown-adjacent service obligation and is already covered by the Brand abuse and Dark Web Monitoring sheets. The CTEM functional requirememt set in the RFP are not in sync with required technical compliance asked in Appendix 1A. Request the Bank to move this clause to Threat Intel Feed section." Request the Bank relocate this item to Appendix 1C, or confirm that it is satisfied by the takedown service procured under the Brand Protection line.	Please refer addendum for revised clause
494	Appendix 1A, page 19	Appendix 1A - CTEM	CTEM item 35	The solution should detect malicious files, reconnaissance activity, automated attack tools, and target lists	Detection of malicious files, reconnaissance activity, automated attack tools and target lists is endpoint and network detection telemetry. The Bank has separately specified XDR at section 7.3.4, NDR at section 7.3.5 and a Threat Intelligence Platform at section 7.3.7 for these outcomes. It seems the CTEM functional requirememt set in the RFP are not in sync with required technical compliance asked in Appendix 1A. Request the Bank relocate this item to the relevant solution sheet, as CTEM solution should not be consuming any detections from those platforms and only validation through integration satisfies the requirement. The CTEM is not supposed to be anothe detection layer on top of already so many individual Detetcion and protection controls implemented or part of this RFP. CTEM is asked as unifying layer for Threat nd Rlsk exposire management at organizationl level	Please refer addendum for revised clause
495	Appendix 1A, page 19	Appendix 1A - CTEM	CTEM item 38	The solution should be deployed agentlessly, without requiring sensors or agents on endpoints, servers, or network appliances	This item requires an agentless deployment without sensors or agents, which directly contradicts the Master Deployment Matrix at section 7.2.1 requiring Bank-hosted CTEM components in N plus N Active-Active configuration at DC and DR, and contradicts the Breach Attack Simulation sheet at Appendix 1C item 8 which requires simultaneous execution of an attack chain across multiple endpoint agents. Request the Bank confirm which architecture is required and reconcile these three clauses.	Please refer addendum for revised clause
496	Appendix 1A, page 19	Appendix 1A - CTEM	CTEM item 39	The solution should integrate via APIs with the existing security stack including NGFW, WAF, XDR, and UEM platforms and other relevant security controls.	Request the Bank publish the make and model of the next generation firewall, web application firewall, XDR and unified endpoint management platforms in use, so that bidders can confirm connector availability rather than warranting integration with an unspecified estate.	Details shall be shared with the successful bidder

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
497	Appendix 1A, page 19	Appendix 1A - CTEM	CTEM item 47	The solution should support cross-platform IoC enforcement across the security stack	The CTEM functional requirememt set in the RFP are not in sync with required technical compliance asked in Appendix 1A. Enforcement of indicators of compromise across the security stack is an orchestration and response function not a CTEM framework capaability. The Bank has separately specified SOAR at section 7.3.2 for exactly this outcome. Request the Bank to move this clause to Threat Intel Feed section." Pushing enforcement actions onto production security controls from an exposure management platform also bypasses the orchestration and change control layer the Bank is procuring. Request the Bank relocate this item to the SOAR sheet, or restate it as publication of indicators to the SOAR platform for enforcement.	Please refer addendum for revised clause
498	Appendix 1A, page 19	Appendix 1A - CTEM	CTEM item 48	The solution should assess and harden network, endpoint, and operating system security controls	Assessment of network, endpoint and operating system control posture is consistent with exposure management, but hardening those controls is a configuration change on production systems. Request the Bank split this item so that assessment and recommendation are scored as a CTEM capability and hardening is assigned to the solution or team that owns the control. Move the hardening part of relevant solution remediation teams rather than CTEM solution doing the hardeneing	Please refer addendum for revised clause
499	Appendix 1A, page 19	Appendix 1A - CTEM	CTEM item 50	The solution should support custom protections tailored to the organization's environment	The term custom protections is not defined and could mean custom detection content, custom validation scenarios or custom enforcement policies, which are materially different capabilities owned by different solutions. Request the Bank define what is meant by custom protections for the purposes of this item.	Custom protection here refers to custom rules, critieria/scoring/metrics or policies etc.
500	Appendix 1A, page 19	Appendix 1A - CTEM	CTEM item 51	The solution should apply virtual patching/compensating controls/exposure mitigation mechaism to the firewall and other security systems through integration with relevant security controls.	Applying virtual patching or compensating controls to the firewall and other security systems is a configuration change on production perimeter devices. In a mature organization like banking sector, this is an intrusion prevention and/or SOAR function, it conflicts with the Bank's own change management controls/policies, and it exposes the Bank to availability risk from an automated action originating in an exposure platform for which the job of virtual patching or mitigating control enforcment is not the role. CTEM is for monitoring and assessment of the overall exposures from Threats and vulnerabilities across bank not used as a compensating or mitigating control plane.. Request the Bank restate this item as recommendation of compensating controls with handover to the owning platform for enforcement, or relocate it to the SOAR sheet.	Please refer addendum for revised clause
501	Appendix 1A, page 20	Appendix 1A - CTEM	CTEM item 57	Upon demand, the vendor should provide a dedicated Customer Success Manager as a single point of contact for onboarding and ongoing support	A dedicated Customer Success Manager is a contractual service commitment and cannot be recorded as standard product functionality. Request the Bank relocate this item to Appendix 1C, and confirm whether the named individual must be provided by the OEM or may be provided by the System Integrator. Request Bank to add the commercial line Item for this requirement	No Change, Please be guided by the RFP
502	Appendix 1A, page 20	Appendix 1A - CTEM	CTEM item 67	The vendor to provide a mechanism to report security incidents identified through the platform and receive prompt response and guidance from the incident response team	Provision of an incident response team is a professional service, and the Bank is separately procuring incident response capability through the NextGen SOC operations and facility management scope. CTEM can be accessed by IR teams during investigations but CTEM cannot invoke reponse for IR team. The CTEM functional requirememt set in the RFP are not in sync with required technical compliance asked in Appendix 1A. Request the Bank relocate this item to Appendix 1C, or confirm that escalation to the System Integrator's SOC satisfies the requirement and is handled out from the solution.	Please refer addendum for revised clause
503	Appendix 1A, page 20	Appendix 1A - CTEM	CTEM item 68	The solution should support MFA for administrative access, role-based access control, and SSO integration	Request the Bank confirm the single sign-on protocol required, whether SAML 2.0 or OpenID Connect, name the identity provider in use, and confirm that federation of administrative access to the Bank's identity provider satisfies both the multi-factor authentication and the single sign-on elements of this item.	No Change, Please be guided by the RFP
504	Appendix 1A, page 1	Appendix 1A	Instruction 1	Bidder must mandatorily mention the exact page number and clause or section reference from their submitted technical proposal or OEM product documentation which demonstrate compliance with each criteria (specification). Any Response marked as compliance without a valid page reference/section reference, shall be treated as in-complete and may be liable for rejection/scoring penalties.	Software delivered as a service is frequently documented through online product documentation and release notes rather than a paginated manual. Request the Bank confirm that a reference to an online documentation article with its title and uniform resource locator, or a signed OEM confirmation letter citing the relevant capability, is acceptable evidence in place of a printed page number.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
505	Appendix 1A, page 1	Appendix 1A	Instruction 2	Any feature or functionality of the proposed solution that is described in the RFP/FRS as 'the solution should support' or 'the solution should have the capability' shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features.	Several items in the CTEM sheet describe analyst services, publication schedules and support commitments rather than product features. Request the Bank confirm how the Day 1 availability obligation applies to such items, and whether recurring analyst services are to be priced within the CTEM product cost or within the offsite services cost.	No Change, Please be guided by the RFP
506	Appendix 1A, page 1	Appendix 1A	Instruction 4	In case bidder has provided the response which is neither 'S' or 'C'. The requirement shall be considered as 'No' or 'N', the bid shall be liable for rejection.	Request the Bank clarify whether a single N response results in rejection irrespective of the aggregate compliance score achieved, or whether the bid remains responsive provided the sheet still meets the 85 percent threshold under eligibility criterion 25. The distinction determines how bidders must answer items that are genuinely inapplicable to their delivery model.	Yes, N/Not Available/ or any other response other than S or C shall lead to rejection of bid
507	Appendix 1A, page 2	Appendix 1A	Cloud deployment requirement 1	Cloud must be hosted in India, and there should be no network and data sharing/replication to any datacenter/office outside the boundaries of India.	Dark web monitoring, brand protection and threat intelligence production depend on global collection, crawling and analyst infrastructure that necessarily operates outside India. Request the Bank confirm that this requirement applies to the Bank's data at rest and in process and to the tenant serving the Bank, and that the provider's global collection and intelligence production infrastructure may operate outside India provided no Bank data is exported.	No Change, Please be guided by the RFP
508	54	7.4	Sub-clause a	In alignment with the regulatory guidelines and advisories, internal information security governance requirements, the Bank proposes to subscribe (Solution licenses are not to be procured) required to a set of specialized, off-site cyber services.	The Phishing Simulation sheet at Appendix 1C item 23.5 requires updates and upgrades of an on-premise platform and item 23.7 requires that no Bank data be stored at the vendor location with storage restricted to the Bank network. An offsite subscribed service procured without licences cannot also be an on-premises platform. Request the Bank state the intended delivery model and align those items with this clause.	Please refer addendum for revised clause
509	56	7.4.5	Anti-Phishing service description	The Bidder shall provide offsite continuous anti-phishing monitoring and response services for detection, analysis for phishing attacks targeting the Bank, its employees, customers, executives, digital assets, domains, and online channels.	The corresponding compliance sheet at Appendix 1C specifies a secure email gateway, covering mail transfer agent forwarding, email quarantine, enforced Transport Layer Security, an impostor classifier and end user email reporting and remediation, across 113 items and 1130 marks. That sheet does not assess the external phishing detection and response service this clause describes. Request the Bank align the compliance sheet with this clause, or separate email security into a distinct line item with its own scope, bill of material entry, Manufacturer Authorisation Form and credential requirement.	Please refer to the relevant Addendum for updated specfications
510	32	7.2.2	Services table note	For all the above Offsite Services, the Delivery Model shall be Managed Service. Any agents, sensors, collectors, connectors or other components required for the collection of logs, telemetry, data or other information necessary for providing the respective Managed Service shall be provided, deployed, configured, maintained and supported by the Service Provider as part of the Managed Service and shall be included in the quoted Managed Service cost.	The Breach Attack Simulation sheet requires simultaneous execution across multiple endpoint agents, which implies deployment of agents across the Bank's estate at no separate cost, yet no endpoint count is stated for this service. Request the Bank state the number of endpoints and zones/CIDR ranges on which breach and attack simulation agents are to be deployed, so that the cost can be quoted rather than assumed.	Details shall be shared with the successful bidder
511	Appendix 1C, page 10	Appendix 1C - Breach Attack Simulation	Breach Attack Simulation item 8	The solution must allow the execution of simulations on multiple agents simulataneously. An attack chain must be executed on multiple endpoints agents at the same time to provide unique attack specific insights across the deployed agents in the organisation.	This item mandates an agent-based architecture, which contradicts Appendix 1A CTEM item 38 requiring an agentless deployment without sensors or agents. Request the Bank reconcile the two clauses, state the number of agents to be deployed, and confirm whether validation architectures that achieve equivalent coverage without a persistent endpoint agent are acceptable.	No Change, Please be guided by the RFP, the requirement is pertainign to BAS and should be complied by BAS Services OEM
512	Appendix 1C, page 10	Appendix 1C - Breach Attack Simulation	Breach Attack Simulation item 9	The solution must provide detailed steps, Indicators of Compromise, IoBs for all the simulation activity performed including but not limited to Process Creation, Service Creation, File Downloads, Network Connection, WMI Queries, Registry Key Modifications, Command Execution, and new threads created with appropriate data to track the attack timeline.	Typoically this is telemetry generated by the security controls and can be integrated with CTEM tool for validating the simulation actions and their corresposbnding logs and events. The host-level artefacts listed are derived from an endpoint agent. Request the Bank confirm whether equivalent evidence correlated from the Bank's existing XDR and SIEM telemetry satisfies this item, since the Bank is separately procuring both platforms under this RFP.	No Change, Please be guided by the RFP, the requirement is pertainign to BAS and should be complied by BAS Services OEM
513	Appendix 1C, page 10	Appendix 1C - Breach Attack Simulation	Breach Attack Simulation item 10	The solution should provide a detailed report on the vulnerabilities/security gaps identified through automated red teaming and summarized report which can be downloaded in PDF, Excel, CSV, Word formats.	The functional requirememt set in the RFP are not in sync with required technical compliance asked in Appendix 1A. The Red teaming exercise are covered in separate CART section. Request the Bank confirm to move this requirement in Red team requirements rather than BAS.	No Change, Please be guided by the RFP
514	Appendix 1C, pages 10-11	Appendix 1C - Breach Attack Simulation	Sheet total	The Breach Attack Simulation compliance sheet contains 11 items and a total of 110 marks.	Under eligibility criterion 25 a C response scores 3 against a maximum of 10, so each C costs 7 marks. On a 110 mark sheet a bidder may record at most two C responses before falling below the 85 percent threshold, whereas the CTEM sheet permits 14, the Dark Web Monitoring sheet 13 and the Phishing Simulation sheet 16. The eligibility gate is therefore materially harsher for this service than for any other for reasons unrelated to capability. Request the Bank normalise the threshold across sheets, or expand the item set for this service so that the gate is proportionate.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
515	Appendix 1C, page 9	Appendix 1C - Attack Surface Management	Attack Surface Management item 42	The solution shall support Multi-Factor Authentication (MFA), role-based access control and integration with enterprise identity providers of the bank	Request the Bank name the enterprise identity provider to be federated with and the protocol it exposes, and confirm that federation through a standard protocol satisfies the multi-factor authentication element of this item.	No Change, Please be guided by the RFP
516	Appendix 1C, page 21	Appendix 1C - Dark Web Monitoring	Dark Web Monitoring item 24	Monitor MX, SPF, DKIM and DMARC changes for suspicious domains.	Monitoring of mail exchanger, sender policy framework, DomainKeys Identified Mail and domain-based message authentication records is an email authentication posture function rather than a dark web intelligence function, and it is also part of requirements in the Phishing Simulation sheet at item 23.2 as an additional requirement. All three solution areas should not supply same functionality and it is very confusing which solution will be the final owner upon deployment. Request the Bank confirm which service line owns this requirement so that it is not procured twice.	No Change, Please be guided by the RFP
517	Appendix 1C, page 21	Appendix 1C - Dark Web Monitoring	Dark Web Monitoring item 25	Provide Passive DNS intelligence and historical DNS resolution.	Request the Bank confirm whether passive domain name system intelligence must be a native capability of the proposed solution or whether it may be delivered through integration with a specialist passive DNS provider or with the Bank's Threat Intelligence Platform.	No Change, Please be guided by the RFP
518	Appendix 1C, page 21	Appendix 1C - Dark Web Monitoring	Dark Web Monitoring item 28.3	IRC	Internet Relay Chat is named as a mandatory collection source. Request the Bank confirm that the requirement is for coverage of real-time messaging channels used by threat actors generally, and that current-generation platforms such as encrypted messaging applications satisfy the intent, since Internet Relay Chat is no longer a primary channel.	No Change, Please be guided by the RFP
519	Appendix 1C, page 21	Appendix 1C - Dark Web Monitoring	Dark Web Monitoring item 28.9	Credit Card Store	Request the Bank confirm the expected handling of payment card data discovered in criminal marketplaces, specifically whether card numbers are to be surfaced to the Bank in full, whether they must be masked or tokenised in accordance with section 7.4 sub-clause d, and through what channel such findings are to be transmitted.	No Change, Please be guided by the RFP
520	Appendix 1C, page 21	Appendix 1C - Dark Web Monitoring	Dark Web Monitoring item 33	Detect fraudulent mobile applications across major application marketplaces.	Detection of fraudulent mobile applications is also required in the Brand abuse sheet at items 13, 19 and 24. It should be part of Dark web monitoring typically Request the Bank confirm which service line owns mobile application impersonation monitoring so that it is not procured and credentialled twice.	No Change, Please be guided by the RFP
521	Appendix 1C, page 22	Appendix 1C - Dark Web Monitoring	Dark Web Monitoring item 35	Support coordination with CERT-In, RBI, Law Enforcement Agency(LEA) and authorized agencies.	Coordination with regulators and law enforcement agencies is a service obligation rather than a platform capability, and the Bank ordinarily leads such engagement itself. Request the Bank define the expected role of the service provider, specifically whether the provider is to prepare evidence packages for the Bank to submit or to engage the agencies directly on the Bank's behalf.	No Change, Please be guided by the RFP
522	Appendix 1C, page 22	Appendix 1C - Dark Web Monitoring	Dark Web Monitoring item 41	Takedown for phishing sites, malicious domains and rogue applications	Takedown of phishing sites, malicious domains and rogue applications is also required in the Brand abuse sheet at items 7 and 16, and each sheet attracts a separate Manufacturer Authorisation Form, credential and compliance gate. Request the Bank confirm that a single takedown capability and a single unlimited entitlement may satisfy both service lines.	No Change, Please be guided by the RFP
523	Appendix 1C, page 22	Appendix 1C - Dark Web Monitoring	Dark Web Monitoring item 49	Support enrichment using CVE, CVSS v4.0, EPSS, CISA Known Exploited Vulnerabilities (KEV) and other industry-recognized threat intelligence sources.	Request the Bank confirm whether support for the Common Vulnerability Scoring System version 4.0 is mandatory from Day 1 or whether scoring under version 3.1 with a migration commitment is acceptable, since adoption of version 4.0 across intelligence sources remains partial.	No Change, Please be guided by the RFP
524	Appendix 1C, page 22	Appendix 1C - Dark Web Monitoring	Dark Web Monitoring item 50	Monitor and identify supply-chain threats affecting the Bank and critical third-party vendors.	Supply chain threat monitoring requires a defined list of critical third-party vendors to monitor. Request the Bank state the number of critical third parties in scope and confirm whether the Bank will supply the vendor list, since without it the scope of this item is unbounded and cannot be priced.	Details shall be shared with succesful bidder
525	Appendix 1C, page 22	Appendix 1C - Dark Web Monitoring	Dark Web Monitoring item 52	The solution shall support initiation and management of takedown requests for phishing websites, typosquatting domains, and rogue mobile applications. The required takedown licenses shall be provided from Day One as specified by the Bank.	Request the Bank define what constitutes a takedown licence, state the expected annual takedown volume by category, state the target takedown service level by category, and confirm the evidence the Bank will accept as proof of a completed takedown. Also, across service there should be a common take down service asked, so that no duplication or ownership crisis happens during operations.	No Change, Please be guided by the RFP
526	Appendix 1C, page 18	Appendix 1C - Brand abuse	Brand abuse item 7	The bidder should offer unlimited number of take down services during the contract period	An unlimited takedown commitment cannot be priced without a volume expectation. Request the Bank publish the takedown volumes it has experienced over the last three contract years by category, so that bidders can price an unlimited commitment on a rational basis rather than on a worst case assumption.	Please refer addendum for revised clause
527	Appendix 1C, page 18	Appendix 1C - Brand abuse	Brand abuse item 14	The Bidder should report the Bank within 1 hour of detection of phishing/brand abuse website/rogue application with action plan on taking down and other alternative response mechanisms upon Bank's confirmation. The Bidder should be able to take down/shut down the phishing/brand abuse website/rogue application within agreed SLA upon Bank's confirmation, irrespective of geography	A one hour detection to notification obligation is a service level rather than a functional specification and it is not reflected in the service level agreement at section 13. Request the Bank confirm the measurement basis for the one hour window, whether it runs from detection by the provider or from first appearance of the asset, and confirm the penalty regime that applies.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
528	Appendix 1C, page 18	Appendix 1C - Brand abuse	Brand abuse item 16	The Service should support Unlimited takedowns of phishing sites, brand abuse and rogue apps during contract period. The Bidder should be capable of blocking of the phishing sites in web browsers. The bidder needs to have tie-ups with Browser providers such as Google, Mozilla, Microsoft and agencies like Cert-In for blocking the phishing sites	This item requires named commercial relationships with specific browser vendors and with a specific national computer emergency response team. Request the Bank restate the requirement as demonstrated capability to achieve browser-level blocking of phishing sites with a stated service level, evidenced by past performance, irrespective of the mechanism or the counterparties through which it is achieved.	Please refer addendum for revised clause
529	Appendix 1C, page 19	Appendix 1C - Brand abuse	Brand abuse item 22	The Bidder/OEM should be member of Anti-Phishing Working Group (APWG).	Membership of a single named industry body is an eligibility attribute unrelated to functional capability and it narrows the field without improving the outcome for the Bank. Request the Bank delete this item	Please refer addendum for revised clause
530	Appendix 1C, page 19	Appendix 1C - Brand abuse	Brand abuse item 23	The Bidder should have global partnership with domain name registrars, application distribution platforms and ISPs for easier take downs of phishing sites & rogue apps anywhere in the world.	Request the Bank restate this item as a demonstrated ability to effect takedowns across registrars, application distribution platforms and internet service providers internationally, evidenced by past takedown volumes and outcomes, rather than as a requirement for named partnership agreements which are not disclosed by providers.	Please refer addendum for revised clause
531	Appendix 1C, page 19	Appendix 1C - Brand abuse	Brand abuse item 32.2	Baiting	The term baiting is not defined. If it denotes the supply of decoy credentials or data to a fraudulent site in order to track its operator, request the Bank confirm that such activity is authorised under the Bank's policy and under applicable Indian law, and state who authorises each instance, since this is an active measure rather than a monitoring function. Tyoically Decoys come under Deception solution farmework and it needs clarity	Please refer addendum for revised clause
532	Appendix 1C, page 19	Appendix 1C - Brand abuse	Brand abuse item 33	Search engines (like Google, yahoo, bing etc.) listing frauds where the customer care number & branch address of banks is changed/ modified should be continuously tracked and the same should be brought down immediately including True caller and JustDial.	This item names specific search and directory services. Request the Bank restate it as a requirement to effect correction or removal of fraudulent listings of the Bank's customer care numbers and branch addresses across major search engines and directory services, so that the requirement remains valid as those services change.	Please refer addendum for revised clause
533	Appendix 1C, page 19	Appendix 1C - Brand abuse	Brand abuse item 34	Prompt submission of enforcement notices and for the removal of rogue or infringing applications	Submission of enforcement notices is a legal function. Request the Bank confirm whether the service provider is expected to issue notices in its own name, in the Bank's name under a power of attorney, or to prepare notices for issue by the Bank's legal function.	Please refer addendum for revised clause
534	Appendix 1C, page 19	Appendix 1C - Brand abuse	Brand abuse item 37	Bidder should be able to identify and report to the bank if access to blocked ports on a webserver is sought by an external user.	This requirement describes perimeter traffic monitoring and the identical sentence also appears in the Threat Hunting Services sheet at item 15. A brand protection provider has no visibility of connection attempts to the Bank's blocked ports unless the Bank supplies firewall telemetry. Request the Bank delete this item from the Brand abuse sheet, or relocate it to the NDR or SIEM specification.	Please refer addendum for revised clause
535	Appendix 1C, page 6	Appendix 1C - Threat Hunting Services	Threat Hunting Services item 2	Collect logs from key log sources in co-ordination with the bank.	Section 7.4.8 states that the service is delivered remotely using mutually agreed mechanisms for accessing logs and telemetry made available by the Bank. Request the Bank confirm that log source onboarding, parser development and collection infrastructure remain the responsibility of the Bank and the SIEM OEM, and that the threat hunting provider consumes the telemetry the Bank makes available rather than deploying its own collection.	No Change, Please be guided by the RFP. The requirement shall be interpreted in accordance with the scope and functionalities specified under Section 7.4.8 – Threat Hunting Services, Appendix 1C. The Threat Hunting Service is intended to provide proactive, hypothesis-driven and intelligence-led technical threat hunting across the Bank's IT and security ecosystem. The service may utilize relevant telemetry and logs available through the Bank's SIEM, as well as other applicable security technologies and data sources, for identifying known and unknown threats,
536	Appendix 1C, page 6	Appendix 1C - Threat Hunting Services	Threat Hunting Services item 15	Bidder should be able to identify and report to the bank if access to blocked ports on a webserver is sought by an external user.	This requirement describes perimeter traffic monitoring rather than threat hunting, and the identical sentence appears in the Brand abuse sheet at item 37. Request the Bank delete this item from the Threat Hunting Services sheet, or relocate it to the NDR or SIEM specification.	Please refer addendum for revised clause
537	Appendix 1C, page 23	Appendix 1C - Phishing Simulation	Phishing Simulation item 14	The bidder shall be capable of performing vishing exercises in both automated and manual methods. The automated approach shall support scalability in conducting vishing campaigns through Bidder's infrastructure/gateway. For conducting vishing using manual approach, each exercise shall be targeted for 100 employees per month.	Request the Bank confirm the total number of employees in scope for voice phishing campaigns per contract year, since the manual approach is capped at 100 employees per month and the automated approach is stated to be scalable, and the two together determine the cost.	The Bidder shall support the vishing volumes specified in the RFP. For manual vishing, the stated requirement of 100 employees per month shall apply. Automated vishing shall support the required campaign population and scalability as specified by the Bank.
538	Appendix 1C, page 23	Appendix 1C - Phishing Simulation	Phishing Simulation item 16	The bidder shall conduct Smishing exercises based on the frequency and number of target employees defined by the Bank. The bidder shall provide, maintain and manage an independent SMS gateway to perform smishing activity as per bank's requirement. The bidder shall maintain adequate security measures to protect Bank's data including any PII information submitted by users during the activity.	Request the Bank confirm the annual volume of simulated messages expected through the provider's independent short message service gateway, and confirm whether the gateway must be hosted in India.	**Please refer addendum for revised clause** **Clarification**:The Bidder shall assess the Bank's requirements and size the SMS gateway/service accordingly. The required target population and frequency shall be as per Bank requirements during the contract period.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
539	Appendix 1C, page 25	Appendix 1C - Phishing Simulation	Phishing Simulation item 23.1	The bidder shall perform review of Email solution twice in a year from Cert-IN empaneled organization and compliance verification shall be conducted within 2 months from the report submission.	Review of the email solution by a CERT-In empanelled organisation is an audit service that falls outside phishing simulation. Request the Bank confirm whether this review is to be performed by the phishing simulation provider, by a separately engaged empanelled auditor, or by the System Integrator, and confirm which party bears the cost.	Please refer addendum for revised clause
540	Appendix 1C, page 25	Appendix 1C - Phishing Simulation	Phishing Simulation item 23.5	The bidder should perform updation of new features and upgradation of on-premise platform automatically from time-to-time.	This item refers to an on-premise platform, whereas section 7.4 states that the Bank proposes to subscribe to offsite services and that solution licences are not to be procured. Request the Bank confirm the intended delivery model and, if an on-premises component is required, state the infrastructure the Bank will provide and confirm that the licence is to be quoted.	Please refer addendum for revised clause
541	Appendix 1C, page 25	Appendix 1C - Phishing Simulation	Phishing Simulation item 23.7	For Phishing activity, the bidder should not store any bank data in vendor location, data storage shall be restricted only on Bank network. The bidder should ensure that the data at rest and in motion shall be encrypted.	A requirement that no Bank data be stored at the vendor location and that storage be restricted to the Bank network is incompatible with an offsite managed service delivered through a centralised platform, as required by section 7.4.4. Request the Bank confirm the intended delivery model, and if offsite delivery is intended, restate this item as a data residency and encryption requirement rather than a prohibition on processing outside the Bank network.	Please refere addendum for revised clause
542	Appendix 1C, page 24	Appendix 1C - Phishing Simulation	Phishing Simulation item 21.1	The platform should include mandatory training modules to train the employees who have been phished.	Security awareness training with a learning management system, content library, assessment and certification is a distinct product category from phishing simulation and is not described in section 7.4.4 of the scope of work. Request the Bank confirm whether a security awareness training platform is within scope, and if so, separate it as its own line item with its own bill of material entry, Manufacturer Authorisation Form and credential requirement.	Mandatory training modules for employees who are identified as having failed/phished during the exercise are within the scope of the Phishing Simulation service.
543	Appendix 1C, page 13	Appendix 1C - Anti-Phishing Services	Anti-Phishing Services item 16.4	The solution should be having Intel source which processes more than 3.4 Trillion Mails in a Year. This is to enable having a good threat intel source to avoid zero day attack vectors.	A threshold expressed as a specific annual message volume processed by the intelligence source is a proprietary metric published by a single vendor and is not independently verifiable. Request the Bank delete the numeric threshold and restate the requirement as demonstrable large-scale email threat telemetry with a described collection basis.	Please refer to the relevant Addendum for updated specfications
544	101-102	10.2	Criterion 5	The bidder should be an authorized representative/ partner/ reseller of OEM in India. MAF should be submitted from 14 solution OEMs and 9 services OEMs, on the official letterhead of the respective OEM, signed by an authorised signatory having the authority to bind the OEM.	Request the Bank confirm that a single Manufacturer Authorisation Form issued by one OEM, listing every solution and service line item that OEM addresses, is acceptable in place of separate letters for each line item, provided each line item is separately and clearly identified within the consolidated letter.	The OEM Declaration shall be submitted by the respective OEM. An OEM may submit a single consolidated annexure covering and highlighting all the relevant details, declarations, and information pertaining to the respective solution(s) being offered as part of this RFP, along with the Bidder's submission.
545	117-120	10.2	Criterion 22	The proposed OEM solution should have been implemented in at least one verifiable client in India. Credential is to be submitted for the following solutions: CNAPP, CWPP, CTEM.	As CTEM Framework is very new and Solutions for CTEM platform are new to market, the availability of dedicated CTEM platform solutions with the Framework applicability and feature functionalities are not yet deployed widely acrioss the globe. In view of this we seek relaxation for this reference. The Claims of references from vendoirs who have solutions in other main areas like VA/VM/BAS and claiming to be CTEM paltform are not CTEM designed platfiorms, they are taking advantage of the common functioinalities like VM/BAS to claim the solution category. However, their references are from their main lines of business only. The regulated sector has just published few RFP's on dedicated CTEm category and are yet to be awarded so this clause needs revisit as requested below. Request the Bank that the client for a CTEM credential may be relaxed to be had from any sector and not restricted to banking, financial services or government. Also, confirm that a deploymen or True CTEM platform with all framework caopabilities may be presently under implementation with a client-issued project status certificate is acceptable, consistent with the evidence list permitted under criterion 19.	No Change, Please be guided by the RFP
546	120-122	10.2	Criterion 23	The proposed OEM services should have been implemented in at least one (1) PSU/ PSE/ Government Organizations / BFSI in India. Credential is to be submitted for each of the nine services.	Several of the nine services can be delivered natively from a single platform. Request the Bank confirm that one production deployment may evidence the credential requirement for each service line that the deployment demonstrably delivered, and that proposing multiple service lines from a single OEM will not be treated as reduced credential strength or as non-compliance or scoring methodology changes.	Yes. Where a single OEM natively provides multiple solution categories, the same credentials may be considered for each applicable category, provided the submitted documents clearly establish the required scope for each category.
547	122-123	10.2	Criterion 24	Compliance Confirmation from respective solution and services OEM. Declaration in the format as mentioned in Annexure 18. FRS and TRS compliance sheet (Excel) are to be submitted along with the self-declaration.	Request the Bank confirm that a single Annexure 18 declaration per OEM covering all line items that OEM addresses is acceptable, rather than a separate declaration for each line item.	The OEM Declaration shall be submitted by the respective OEM. An OEM may submit a single consolidated annexure covering and highlighting all the relevant details, declarations, and information pertaining to the respective solution(s) being offered as part of this RFP, along with the Bidder's submission.
548	123	10.2	Criterion 25	The proposed product should have minimum functional compliance score of 85% for each of the following solutions and services. Each product/solution shall be evaluated independently, and the compliance score shall be computed separately for each product/solution.	Because a C response scores 3 against a maximum of 10, the number of permissible C responses varies from 2 on the Breach Attack Simulation sheet to 16 on the Phishing Simulation sheet purely as a function of sheet size. Request the Bank confirm whether this variation is intended, and consider applying the threshold to the aggregate of the solutions and services proposed by a single OEM.	No Change, Please be guided by the RFP. Each product/solution shall be evaluated independently, and the compliance score shall be computed separately for each product/solution.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
549	127	10.2	Note d	Either the Principal/OEM or its authorized agent may submit a bid for a given item/product under this RFP. However, both the Principal/OEM and its authorized agent shall not be permitted to submit bids simultaneously for the same item/product in the same RFP. Further, where an agent is authorized to represent a Principal/OEM, the same agent shall not submit bids on behalf of more than one Principal/OEM for the same item/product.	Request the Bank confirm that an OEM may authorise more than one System Integrator to propose its product in this RFP, and that the restriction operates only on the bidding entity, since an OEM has no visibility of which System Integrators intend to bid.	Yes, your understanding is correct
550	127	10.2	Note j	Deployments shall be considered valid only if the solution has been used for its intended function in a production environment. Tests, pilot, or non-production deployments shall not be accepted.	Request the Bank confirm the evidence it will accept to demonstrate production use, and confirm that a client acceptance or go-live certificate is sufficient without requiring disclosure of the client's production configuration.	No Change, Please be guided by the RFP
551	128	10.2	Note m	Experience must be showcased separately for each solution category, with clear evidence that each solution has been deployed as a standalone solution and not merely as a feature or component of another solution.	Integrated exposure management platforms deliver attack surface management, exposure validation and threat hunting as separately licensable, separately priced and separately deployable subscription modules. Applied literally this note excludes such platforms while favouring assemblies of point products, which runs against the Bank's stated objective at section 7.3.14 of an integrated unified risk dashboard. Request the Bank confirm that a separately licensable and separately priced module qualifies as standalone evidence where it is evidenced as deployed in production and used for its intended function.	Yes. Where a single OEM platform natively provides multiple solution categories, the same credentials may be considered for each applicable category, provided the submitted documents clearly establish the required scope for each category.
552	109	10.2	Criterion 18	To ensure conflict of interest the successful bidder or its subsidiary or its associate or sister company or its holding company should not be the IT Security vendor of the bank under the existing or new contract.	Request the Bank confirm that this restriction applies to the bidding entity and its group companies only, and does not extend to a solution or service OEM whose product may be proposed by different System Integrators in this and other Bank procurements.	Yes, this particular Clause is for bidder
553	126	10.2	Note on the parallel RFP	In the event a Bidder participates in both the NextGen SOC RFP and IT Security solution (PartA/PartB and Firewall) and services RFP and is declared the successful bidder in either of the RFPs, such Bidder shall be deemed ineligible for award in the other RFP.	Request the Bank confirm that this restriction applies to the bidding entity only and not to OEMs whose products may be proposed by different bidders in both procurements, and confirm the sequence in which the two commercial evaluations will be conducted so that bidders can assess the risk of participating in both.	Yes, this particular Clause is for bidder
554	131	10.3	Criterion 4, scoring category	Category: a. Point 1: = 1 Client. b. Point 2: > 2 Client.	A bidder holding exactly two client credentials falls between the two bands and appears to score nothing. Request the Bank correct the bands to one client and two or more clients, or state how exactly two credentials will be scored.	No Change, Please be guided by the RFP, RFP Clearly highlights the following Category: a. Point 1: = 1 Client b. Point 2: > 2 Client
555	132	10.3	Criterion 5, scoring category	Category: a. Point 1: = 1 Client. b. Point 2: > 2 Client. Credential is to be submitted for each of the following solutions: CNAPP, CWPP, CTEM.	A bidder holding exactly two client credentials for CNAPP, CWPP or CTEM falls between the two bands and appears to score nothing. Request the Bank correct the bands to one client and two or more clients, or state how exactly two credentials will be scored.	No Change, Please be guided by the RFP, RFP Clearly highlights the following Category: a. Point 1: = 1 Client b. Point 2: > 2 Client
556	133	10.3	Criterion 6, scoring category	Category: a. Point 1: 1 Client. b. Point 2: >2 Clients.	A bidder holding exactly two client credentials for a service falls between the two bands and appears to score nothing. Request the Bank correct the bands to one client and two or more clients, or state how exactly two credentials will be scored.	No Change, Please be guided by the RFP, RFP Clearly highlights the following Category: a. Point 1: = 1 Client b. Point 2: > 2 Client
557	133-134	10.3	Criterion 7, Technical presentation	Technical presentation and Responses provided during the session will be considered part of the Technical Bid and are contractually binding.	Request the Bank confirm that only written responses submitted or confirmed in writing following the presentation are contractually binding, so that a verbal answer given under time pressure does not become a contractual obligation without review.	No Change, Please be guided by the RFP
558	135	10.4	Commercial Evaluation Criteria	The bidder quoting the lowest evaluated Total Cost of Ownership (TCO), as determined by the Bank, shall be ranked as L1 (Lowest Bidder). Award of Contract shall be considered for the bidder ranked L1.	Request the Bank confirm that technical marks operate purely as a qualifying threshold at 80 of 100 and carry no weight in the award decision, and that no quality and cost based composite score will be applied.	Yes, Award of Contract shall be considered for the bidder ranked L1 not QCBS
559	136	11	Right to Reduce / Descope Solution Components Prior to Award	Any subsequent descope shall not be used to alter the ranking/L1 position of bidders or to conduct post-bid price negotiations. Such reduction, modification or descope shall not create any liability or obligation towards the Bidder.	Where a descoped component is a licensable module of an integrated platform, removing it can change the unit economics of the modules that remain. Request the Bank confirm that the bidder may restate the dependent licensing, support and cost implications under the notification mechanism already provided in this section, and that the resulting revised configuration will not be treated as a post-bid price change.	Please refer addendum for revised clause
560	137	12.1	Product Licence Cost, milestone 1	On successful delivery of the licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware. The Bidder is required to submit Delivery proof, OOTB Installation Proof and Invoice of the Product.	For solutions the Bank has itself designated as Cloud SaaS there is no proposed hardware and no on-premises installation event, so this milestone cannot be evidenced as written. Request the Bank define an equivalent milestone for SaaS line items, for example tenant provisioning and access handover confirmed in writing by the Bank.	No Change, Please be guided by the RFP
561	137-138	12.1	Subscription Cost, milestone 3	Subscription Cost (One time license Cost). On successful delivery of the Licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware.	Request the Bank confirm the evidence required to release the first tranche for a subscription delivered as a service, and confirm that out of the box installation proof on hardware is not applicable to such line items.	No Change, Please be guided by the RFP
562	139	12.4	ATS/subscription cost & AMC Cost	Annually in Advance: Upon submission of a Bank Guarantee equivalent to 110% of the annual subscription/Annual technical cost of the respective product, valid for the applicable subscription period; or Quarterly in Arrears.	Request the Bank confirm that the choice between annual in advance against a bank guarantee and quarterly in arrears rests with the bidder, and confirm that the cost of the bank guarantee is to be included in the quoted price.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
563	261	Annexure 21.2	Item 16, CTEM volumetrics	CTEM: Vulnerability / Exposure Findings - Unlimited. Attack Paths / Exposure Relationships - Unlimited. Users/Endpoints - 12000 scalable to 16000. IPs - 4000.	Exposure management platforms are commonly licensed by asset, by internet-facing asset or by subscription tier rather than by user or endpoint. Request the Bank state the licensing metric it expects to be quoted, confirm whether the figure of 12,000 scalable to 16,000 refers to identities in scope or to endpoints requiring an agent, state how the figure of 4,000 IPs relates to externally discovered assets which are by definition not known in advance, and confirm the commercial treatment of assets discovered beyond these volumetrics.	No Change, Please be guided by the RFP
564	257	Annexure 21.1	Current IT assets	Note: The count of IT & Security Infra as listed above is tentative.	Sizing, licensing and service pricing are derived directly from these counts. Request the Bank confirm the tolerance within which the tentative figures may vary, and confirm the commercial mechanism that applies where actual counts exceed the stated figures during the contract period.	No Change, Please be guided by the RFP
565	26	7.1	Post quantum cryptography readiness	The proposed solution shall support PQC readiness, including support for secure cryptographic mechanisms and standards that facilitate future migration to quantum-resistant cryptography, wherever applicable to the solution.	Request the Bank confirm what evidence satisfies post quantum cryptography readiness at bid stage, specifically whether an attestation of cryptographic agility together with a published migration roadmap is sufficient, or whether implementation of a named post-quantum algorithm suite is required from Day 1.	No Change, Please be guided by the RFP The proposed solutions shall demonstrate a documented roadmap/capability for post-quantum cryptography readiness, including support for migration to applicable NIST-standardized PQC algorithms or approved industry standards as relevant to the solution. The bidder shall disclose current capability, dependencies and roadmap.
566	27	7.1	Key Implementation Responsibilities, clause a	The implementation of each proposed solution, including design, installation, configuration, integration, migration, testing, user acceptance testing (UAT), and Go-Live, shall be performed by the respective OEM. Upon successful implementation, the respective OEM shall provide a certificate confirming that the solution has been deployed by the OEM.	Request the Bank confirm the expected scope of OEM implementation for a solution delivered as a service with no installation event, specifically whether high level design, low level design, integration design, connector configuration, system integration testing and user acceptance testing support, as-built documentation, knowledge transfer and the OEM go-live certificate constitute the complete deliverable set, and whether OEM implementation resources may be delivered remotely.	No Change, Please be guided by the RFP
567	59	7.6	OEM Responsibilities, clause 9	The OEM shall maintain and periodically (Quarterly or as required by regulators) update Software Bill of Materials (SBOM), Cryptographic Bill of Materials (CBOM), Quantum Bill of Materials (QBOM), AI Bill of Materials (AI-BOM), and all dependent components in accordance with applicable CERT-In guidelines.	Request the Bank confirm, for a multi-tenant cloud platform delivered as a service, whether component-level disclosure is limited to the components exposed to or consumed by the Bank rather than the provider's entire internal platform, state the acceptable submission format, and confirm the treatment of commercially confidential dependency information.	The required details as mentioned in the RFP and subsequently sought by the regulatory/statutory bodies from time to time during the contract period is to be provided
568	NA	Threat Intelligence Feed	To be added	TIF Solution must include following feeds: > IP Reputation Data Feed The solution must provide 170K+ records, with an average update frequency of 20 minutes, including contextual information such as category, geolocation, threat score, domains and popularity. > Malicious URL Data Feed The solution must provide 80K+ records, with an average update frequency of 10 minutes, including contextual information such as popularity, geolocation, associated IP addresses, URLs, hosts and domains. > Phishing URL Data Feed The solution must provide 300K+ records, with an average update frequency of 30 minutes, including relevant contextual information such as popularity, geolocation, associated IP addresses, URL, phishing kit, stolen data type and attack type. > Botnet C&C URL Data Feed The solution must provide 400K+ records, with an average update frequency of less than 1 hour, including relevant contextual information such as popularity, geolocation, threat, associated IP addresses, URLs,	Justification: The specifications for the Threat Intelligence Platform and Threat Intelligence Feeds are closely interrelated, and no specific feeds have been defined under the Feed requirements. However, clauses related to Dark Web Monitoring, Brand Monitoring, ASM, etc. appear to overlap with capabilities already requested under separate components. We request reconsideration and rationalization of these overlapping clauses to avoid duplication and reduce the overall TCO. There is no clause explicitly asking for threat intelligence feeds and kind of feeds needed for SOC. This point is added to ensure the Threat Intelligence Feed solution provides sufficiently broad, current, and measurable coverage across the major indicator categories used for proactive blocking and detection, namely IP reputation, malicious URLs, phishing URLs, and botnet C&C infrastructure. Feeds that are not refreshed frequently enough exposes the organization to newly weaponized infrastructure that has already bypassed stale reputation databases.	No Change, Please be guided by the RFP
569	NA	Threat Intelligence Feed	To be added	The Threat Intelligence solution must also provide comprehensive coverage of cyber threats originating from the Eastern hemisphere, with dedicated feeds and intelligence derived from proprietary telemetry and research operations in regions including Russia, China, India, and Cuba. Vendors must demonstrate this coverage through valid proof of locally established research operations or legal entities in these regions	Justification: This point is added because a significant share of advanced, state-sponsored, and financially motivated threat activity relevant to the organization originates from or is operated out of the Eastern hemisphere (Russia, China, India, Cuba, among others). Threat intelligence sourced primarily from Western-centric telemetry and research often has limited visibility into regional campaigns, local-language threat actor communications, and region-specific malware/TTPs. Requiring proprietary telemetry and demonstrable local research operations or legal presence in these regions ensures the intelligence is first-hand and authentic rather than re-packaged third-party data, giving the organization earlier warning and more accurate, actionable intelligence on threats most likely to target it.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
570	NA	Threat Intelligence Feed	To be added	The threat intelligence feeds provider have at least 15+ years of global expertise in malware and APT research. The solution shall provide in-house researched and maintained threat actor profiles with original attribution capability, not sourced or white-labeled from third-party intelligence providers,covering 900+ APT groups and operations monitored.	Justification: This point is added to establish an objective minimum bar for vendor maturity and intelligence quality. A minimum of 15+ years of global malware/APT research experience helps ensure the bidder has the institutional expertise, historical data, and analyst bench strength needed to deliver reliable, high-confidence intelligence. Requiring in-house researched and maintained actor profiles with original attribution (rather than data licensed or white-labeled from a third party) ensures accuracy, accountability, and independent verification of findings, and prevents the organization from indirectly paying twice for the same repackaged intelligence. Specifying coverage of 900+ APT groups sets a clear, measurable benchmark for breadth of coverage, ensuring the selected solution offers comprehensive visibility into the current global threat actor landscape rather than a narrow subset.	No Change, Please be guided by the RFP
571	35 of 122	XDR	4.13	The goal is to minimize the attack surface by continuously monitoring, updating, and provide compensatory controls for vulnerabilities and exploits in the endpoints	We request to modify this clause as below "The goal is to minimize the attack surface by continuously monitoring, updating, and provide visibility for vulnerabilities and exploits in the endpoints" Justification: The term "visibility" is outcome-focused and technology-agnostic, allowing solutions to detect and report vulnerabilities through various mechanisms (signatures, behavioral analysis, real-time scanning, etc.), whereas "compensatory controls" is overly prescriptive and implies specific mitigation techniques that may not be applicable to all vulnerability types or endpoint environments. Changing to "visibility" maintains the security intent while enabling bidders to propose diverse, fit-for-purpose solutions without unnecessary implementation constraints.	No Change, Please be guided by the RFP
572	35 of 122		12	The proposed solution must provide protection against malicious AI application tampering on the endpoints	We request to modify this clause as below "The proposed solution must provide protection against malicious applications tampering on the endpoints" Justification:The "AI" qualifier is overly specific and may exclude non-AI malware threats, creating coverage gaps. The broader term "malicious application tampering" aligns with industry-standard endpoint protection language and ensures comprehensive threat protection regardless of the attack vector or technology employed.	No Change, Please be guided by the RFP
573	36 of 122		15	The proposed XDR solution must provide comprehensive activity data management and search capabilities, including receiving activity data in the form of telemetry, and metadata; feature for automatic query runs and email notifications; threat matching features using Boolean Logic and other criteria; and options to export, **import,** delete, and share saved search queries.	We request to modify this clause as below: The proposed XDR solution must provide comprehensive activity data management and search capabilities, including receiving activity data in the form of telemetry, and metadata; feature for automatic query runs and email notifications; threat matching features using Boolean Logic and other criteria; and options to export, delete, and share saved search queries. Justification:The "import" functionality is not a core operational requirement for XDR activity data management. The primary requirements are exporting queries for backup/sharing, deleting obsolete queries, and sharing queries among team members—all of which are standard XDR capabilities. Import functionality introduces unnecessary complexity, potential security/governance risks from external query sources, and is not universally supported across commercial XDR solutions, thereby limiting vendor options unnecessarily	No Change, Please be guided by the RFP
574	36 of 122		22	The solution should offer options to leverage anti-malware and anti-spyware components stored locally on agents, or signatures stored in-the-vendor cloud	From the operational context and use cases for each deployment option, ensuring continuity of threat protection in all connectivity scenarios. By explicitly defining "when offline" (local components) and "when online" (cloud signatures), the clause removes ambiguity regarding the solution's capability to maintain protective coverage during network disconnections while leveraging updated threat intelligence when connectivity is available We request to modify this clause as below "The solution should offer options to leverage anti-malware and anti-spyware components stored locally on agents when offline, or signatures stored in-the-vendor cloud when online."	No Change, Please be guided by the RFP
575	36 of 122		29	The solution Device Control capability must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The solution Device Control capability must support Network Devices, USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, time based device control capabilities allowing admin to define the policy specifically for the endpoint operating systems (Windows 10, 11 or higher).	We request to modify the clause as below: The solution Device Control capability must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The solution Device Control capability must support USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, allowing admin to define the policy specifically for the endpoint operating systems (Windows 10, 11 or higher)to allow the devices as required. Justification: Network Devices are typically managed through enterprise network security controls and firewalls rather than endpoint Device Control, and time-based controls create unnecessary operational complexity and maintenance overhead. The modified clause focuses on high-risk local device vectors (USB, Mobile Storage, Bluetooth, Modems) that pose direct security threats to endpoints, while allowing flexibility for organizations to enable specific devices based on business requirements.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
576	37 of 122		43	The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature or through seamless integration with a third-party sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data	We request to amend this clause as below: The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data. Justification: To ensure operational independence and reduce implementation complexity, the organization requires native sandbox functionality built into the core solution rather than relying on third-party integrations, which introduce external dependencies, potential single points of failure, and increase support overhead. This modification mandates that bidders deliver complete sandboxing capability as an integrated component from day 1, ensuring seamless functionality, consistent vendor accountability, and simplified maintenance and support operations without external vendor coordination.	Please refer addendum for revised Clause
577	38 of 122		57	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	We request to amend this clause as below: The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture or 99.9% availability SLA distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead. Justification: The modification provides architectural flexibility while maintaining the Bank's core availability objective. Not all qualified SaaS vendors employ Active-Active multi-AZ architecture; however, industry-standard 99.9% SLA meets enterprise-grade requirements and enables broader vendor participation without compromising operational resilience. This alternative approach is vendor-agnostic, measurable, and backed by contractual guarantees rather than architectural prescriptions.	Please refer Addendum for revised clause
578	37 of 122		42	The proposed solution should provide recommended actions to address and mitigate threats detected on endpoints. These remediation suggestions should be informed by forensic data collected from endpoints and detailed analysis performed by the solution to enhance threat response and resolution.	To ensure accurate cost proposals and licensing calculations, please clarify the estimated forensics data volume requirements: a) What is the expected monthly forensics data volume (in GB) that the solution must support? b) What is the planned retention period for forensics data? c) Does this volume include forensics data from all sources (endpoints, servers, cloud workloads, network) or specific sources only? This clarification will enable all bidders to calculate appropriate licensing models and provide consistent cost estimates	Details shall be shared with the successful bidder
579	54 of 122	Cloud Security	4	The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud envirionment like AWS/Azure/GCP/Meghdoot, AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.	We request to modify this clause as below The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud envirionment like AWS/Azure/GCP/ AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports. Justification: Meghdoot is a comprehensive open-source cloud suite, but bringing it up to PSB requirements demands significant development and integration effort. To be effective, the target cloud environment must be seamless, eliminating the overhead of custom modifications.	Please refer addenudm for revised clause The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud envirionment like AWS/Azure/GCP, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.
580	Addition of Point as recommendation	Cloud Security	To be Added in Cloud Security	The proposed solution should also support the File scanning with no limitation on file/object type or size covering application across organisation. This should include but is not limited to Amazon Simple Storage Service (S3), Amazon FSx amd Amanzon Elastic File System.	Benefit to PSB: Comprehensive file scanning eliminates critical security blind spots across the organization's cloud storage infrastructure, ensuring no malware, ransomware, or sensitive data can be inadvertently stored in S3, FSx, or EFS without detection. By removing file type and size limitations, the solution prevents attackers from bypassing scanning through obfuscation or leveraging uncommon formats, while the multi-storage coverage consolidates security posture across diverse AWS storage services under a single unified policy. This provides unified threat visibility, enables regulatory compliance (HIPAA, PCI-DSS, GDPR), prevents data exfiltration, and protects against insider threats and supply chain compromises affecting cloud-stored data—significantly reducing the risk of ransomware attacks, compliance violations, and unauthorized data exposure.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
581	page 30 of 273	Extended Detection & Response (XDR)	5	Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Cloud (SaaS): HA Deployment aligned with the SLA, RTO & RPO (Refer Section 13). Management Console: Deployed at both Primary and Secondary sites	We request to amend this clause as below: Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Cloud (SaaS): HA Deployment aligned with the SLA, RTO & RPO (Refer Section 13). Justification: In Appendix 1A clause 27 under XDR explicitly mention for SaaS "ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead" Though it's a SaaS based the management console cannot be deployed at both primary and secondary sites.	Please refer addendum for revised clause
582	page 31 of 273	Cloud Workload Protection Platform (CWPP)	13	Cloud (SaaS): Deployment aligned with the SLA, RTO & RPO (Refer Section 13).. Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Management Console: Deployed at both Primary and Secondary sites	We request to amend this clause as below: Cloud (SaaS): Deployment aligned with the SLA, RTO & RPO (Refer Section 13).. Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Justification: For SaaS solution the management console cannot be deployed at banks primary & secondary site	Please refer addendum for revised clause
583	Page 38 of 122 & Page 38 of 122	XDR	22 to 35	These points are duplicate need to be removed	These points are duplicate need to be removed	No Change, Please be guided by the RFP
584	29, 35 & 259	Sections 7.2.1, 7.2.4.1(b) & 16.21.2		Deception deployment and high-availability topology Section 7.2.1 (Deception Technology): "Any agent/Enforcer/Deceptor Standalone at DC and HA, N+N, Standalone at DR." Section 7.2.4.1(b): "The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active configuration." Section 16.21.2 (Decoy): "All the inline components of the solution must operate in high availability mode. In the event of any component failure, the system should automatically initiate failovers within seconds, ensuring uninterrupted functionality without requiring manual intervention."	The RFP describes the Bank-side deception components as standalone in Section 7.2.1, point no.- 4, but it is also mentioned HA and N+N. We request the bank to kindly clarify that in case we're deploying the solution on-prem, whether Bank needs the solution in Standalone mode/HA mode/N+N mode. Section 16.21.2 (Decoy), point no.-8, Bank has asked that all the inline components of solution should be in HA mode with automatic failover capability. However, the deception solution is not inline. Hence, we request Bank to clarify if they need the Deception Solution in HA. We request the Bank to add on-prem solution also in addition to Cloud/SAAS+Hybrid.	Please refer addendum for revised clause
585	45, 261 & 262	Sections 7.3.6.2(2) & 16.21.3 - Deployment and Data Retention		Backup, restoration and log-retention requirements Section 7.3.6.2(2): "Restore the logs/data from backup for forensic investigation and as per bank requirement without any additional cost." Section 16.21.3: "Duration of the Contract (Monthly Full backup) - Long-Term Storage (LTS) - Entire Duration of the Contract." The RFP further states that applicable Monthly Full Backups shall be migrated to LTS at the Bank's DC & DR and retained for the entire duration of the contract.	We request bank to kindly confirm that if the bank will provide the storage for backup.	No Change, Please be guided by the RFP. Bidder to right size and provide all the required infrastrcuture as per RFP
586	68	Section 7.7 - On-cloud proposed solution OEM Responsibilities, Point 10	"The OEM shall have valid ISO/IEC 27001 certification and SOC 2 Type II report."	Cloud OEM certification requirement	We request the bank to accept ISO/IEC 27001 or SOC 2 Type II or both.	No Change, Please be guided by the RFP
587	29, 32 & 35	Sections 7.2.1, 7.2.3 and 7.2.4.1(b)		Responsibility for providing the Cloud/SaaS environment Section 7.2.1 (Deception Technology): "Cloud (SaaS) + Hybrid" Section 7.2.3: "The solution shall be hosted through a Cloud Service Provider (CSP), either fully as a SaaS service or through a combination of CSP-hosted and Bank-hosted components." Section 7.2.4.1(b): "Deception Technology: The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active configuration. The Cloud/SaaS deployment shall be aligned with the applicable SLA, RTO and RPO requirements."	7.2.4.1(b) We request the bank to kindly add the on-prem implementation option also for the core component of the Deception Solution.	Please refer addendum for revised clause
588	35 & 91	Sections 7.2.4.1(b) and 7.18.1 - Compute Infrastructure, Point 1		Hardware and VM infrastructure for Bank-hosted deception components Section 7.2.4.1(b): "Deception Technology: The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active configuration. The Cloud/SaaS deployment shall be aligned with the applicable SLA, RTO and RPO requirements." Section 7.18.1(1): "Bidders must design, size, supply, implement, maintain and manage suitable compute infrastructure for all the in-scope applications/solutions proposed in the RFP response."	We request the bank to kindly add the on-prem implementation option also for the core component of the Deception Solution.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
589	84	Breach and Attack Simulation (BAS)	Sl. No. 1 - Technical Specification	The solution should simulate Ransomware Attacks	Rationale for change: The clause as drafted is a single unqualified statement that every bidder in this category will mark compliant, so it cannot differentiate responses against the 10 marks allotted. It also does not define what constitutes a ransomware simulation. A ransomware validation exercise is only meaningful to the Bank if the platform reproduces the tradecraft ransomware operators actually use, including vulnerable driver loading to terminate endpoint protection, and does so without causing damage on production assets. The Bank is requested to replace the clause with testable criteria covering safe execution of destructive behaviours, deterministic cleanup, and kernel-level attack testing. Proposed modified clause: The proposed solution must execute structurally authentic attacks with destructive elements neutralised, and must be able to trigger destructive-technique detections without the harmful action (for example, testing volume shadow copy deletion detection without deleting the volume shadow copy). It must provide deterministic cleanup mechanisms, safe for execution on production assets, including backup, restore, and removal of all artifacts across: a. File b. Registry c. Service	No Change, Please be guided by the RFP
590	84	Breach and Attack Simulation (BAS)	Sl. No. 3 - Technical Specification	The ability to simulate infiltration techniques for breaching a network or infecting a host	Rationale for change: "Infiltration techniques" is undefined and cannot be evaluated objectively. Initial access is the stage at which the Bank's email gateway, secure web gateway and web application firewall are tested, and current adversary tradecraft delivers initial access through container formats such as ISO, IMG, MSI, LNK and ZIP, followed by execution that avoids system interpreters in order to bypass AMSI, script block logging and constrained language mode. A clause that names these delivery and execution requirements allows the Bank to compare bidders on demonstrable capability rather than on a general claim. Proposed modified clause: The proposed solution must dynamically generate container-format payloads including ISO, IMG, MSI, LNK, and ZIP variants containing executables, shortcuts, or DLL hijack chains, and deliver them via uniquely generated URLs per simulation to comprehensively validate email gateway, secure web gateway, and WAF filtering against modern initial-access techniques such as ISO-LNK-DLL chains. The simulation agent must execute malicious behaviours and adversary techniques without reliance on system interpreters including PowerShell, CMD, BASH, or SH, validating control effectiveness against modern adversary tradecraft that increasingly avoids interpreter-based execution to bypass AMSI,	No Change, Please be guided by the RFP
591	84	Breach and Attack Simulation (BAS)	Sl. No. 6 - Technical Specification	The solutions should test Security Operations Center (SOC) detection capability of bank by simulating multi-chained payloads with advanced evasion methods including DLL Hijacking, Process Injection, and PPID spoofing for breaching and infiltrating the network.	Rationale for change: The clause names only three evasion techniques and does not state that they must be executed as real behaviours on the asset rather than logged as simulated steps. SOC detection validation succeeds or fails on two things the clause does not capture: whether the payload natively performs modern evasion against the deployed control stack, and whether each technique is available in multiple procedure variants, since a detection that catches one implementation of LSASS credential dumping routinely misses six others. The Bank is requested to expand the clause so that detection coverage is validated across the attacker variant space. Proposed modified clause: The simulation payload execution must natively perform the following techniques as executed behaviours against the deployed control stack: a. EDR unhooking (NTDLL unhooking, direct and indirect syscalls) b. Reflective DLL injection c. Process hollowing d. PPID spoofing e. Command-line argument spoofing f. Fileless in-memory execution For each in-scope MITRE ATT&CK technique, the proposed	No Change, Please be guided by the RFP
592	84	Breach and Attack Simulation (BAS)	Sl. No. 7 - Technical Specification	The solution should have the ability to create custom use cases / simulations attacks according to bank's requirement.	Rationale for change: As drafted the clause is satisfied by a script upload field or by a vendor professional services engagement, both of which leave the Bank dependent on the OEM for every new scenario and carry recurring cost. For the Bank's own security team to build scenarios for proprietary applications and internal workflows, the clause should require a user interface driven attack creator with named configurable parameters. Proposed modified clause: The proposed solution must provide a UI-driven attack creator enabling customer security teams to design custom multi-stage simulations with configurable name, description, MITRE category, execution privileges (User/Admin), payload type (DLL/EXE/Service/ISO/MSI/LNK), and chained secondary behaviours supporting organisation-specific scenario testing for proprietary applications, internal workflows, and bespoke attack hypotheses.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
593	84	Breach and Attack Simulation (BAS)	Sl. No. 8 - Technical Specification	The solution must allow the execution of simulations on multiple agents simulataneously. An attack chain must be executed on multiple endpoints agents at the same time to provide unique attack specific insights across the deployed agents in the organisation.	Rationale for change: The clause states the requirement for simultaneous execution but does not exclude sequential execution presented as a single campaign, which is how several solutions in this category operate. It also does not address the operational prerequisites for running simulations across a bank-scale estate: the agent must be deployable at scale through Group Policy or golden image, must run silently so that branch and business users are not alerted or disrupted, and must update centrally without re-imaging or desk visits. The Bank is requested to make both the concurrency model and the deployment model explicit. Proposed modified clause: The proposed solution must execute a single coordinated attack campaign across multiple agents, business units, and geographies simultaneously, not sequentially (i.e. One Kill chain, run on multiple Endpoint Targets at the same time), producing independent per-agent evidence consolidated into a unified campaign report. Solutions that walk through agents one-by-one cannot realistically validate enterprise-scale concurrent compromise scenarios. The simulation agent must be a lightweight software package suitable for enterprise mass-deployment via Group Policy Object (GPO), golden image baking, or standard endpoint management tooling, requiring no per-host configuration post-installation.	No Change, Please be guided by the RFP
594	84	Breach and Attack Simulation (BAS)	Sl. No. 11 - Technical Specification	The solution should support technical integrations with bank's existing solutions (e.g., SIEMs, ticketing systems, log management, Firewalls, automation/orchestration, analytics solutions, threat intelligence solutions, etc.)	Rationale for change: "Should support technical integrations" is unverifiable and is routinely answered with roadmap commitments or bespoke development quoted after award. For closed-loop validation, where a simulation result is correlated against the alert raised in the Bank's SIEM and a ticket is created automatically, the Bank needs a documented API, automation tooling and pre-built connectors available at the time of bid. The Bank is requested to make the integration requirement specific and verifiable. Proposed modified clause: The proposed solution must expose a RESTful API with publicly available OpenAPI documentation, provide an open-source CLI and SDK for automation, and ship pre-built integrations with major SIEM, SOAR, ITSM, EDR, firewall, and email gateway vendors to enable closed-loop validation of alerts, automated ticket creation, and detection correlation.	No Change, Please be guided by the RFP
595	30	RFP - 7.2 Solution & Services Deployment Model and Their HA Requirement 7.2.1 Solutions – Master Deployment Matrix	6. Network Detection & Response (NDR)	Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Management Console: Deployed at both DC and DR	Different NDR solution works on different redundancy deployment methodology (I.e Active - Active or Active - Passive). Request bank to modify the clause as: Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active/Passive at DC and HA, N+N, Active-Active/Passive at DR. Management Console: Deployed at both DC and DR	Please refer addendum for revised clause
596	45	RFP - Scope of Work 7.3.5 Network detection and response (NDR)	7.3.5.1 Modules, Architecture & Deployment:	Pt 2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Generally NDR solutions are deployed with sole purpose of doing network analysis, threat detection & response and does not have native 2FA capability, so request bank to remove this point. As an alternate as proposed in same point, proposed NDR solution can be integrated with bank's existing MFA solution.	Please refer addendum for the revised clause
597	49	RFP - Scope of Work 7.3.10 Application security testing Tool	7.3.10.1 Modules, Architecture & Deployment:	Pt 2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Generally AST solutions are deployed with sole purpose of scanning the source code, web, api etc and does not have native 2FA capability, so request bank to remove this point. As an alternate as proposed in same point, proposed AST solution can be integrated with bank's existing MFA solution.	No Change, Please be guided by the RFP
598	110	RFP - 10.2 Eligibility Evaluation Criteria	OEM Evaluation Criteria	Pt 19. The proposed OEM SIEM Solution with a minimum capacity of 30,000 EPS or 1.2 TB/day shall have been successfully implemented on cloud in one (1) in India.	For wider participation, we request bank to amend the clause as: The proposed OEM SIEM Solution with a minimum capacity of 5,000 EPS or.2 TB/day shall have been successfully implemented on cloud in any one (1) Govt/PSU customer in India. OR The proposed OEM SIEM Solution with a minimum capacity of 10,000 EPS or.4 TB/day shall have been successfully implemented on cloud in one (1) in India.	Please refer addendum for revised clause.
599	112	RFP - 10.2 Eligibility Evaluation Criteria	OEM Evaluation Criteria	Pt 20. The proposed OEM solution should have been implemented in at least one BFSI is to be submitted for the following solutions: NDR	For wider participation, we request bank to amend the clause as: The proposed OEM solution should have been implemented in at least one BFSI / Govt is to be submitted for the following solutions: NDR	Please refer addendum for the revised clause
600	260	RFP - 16.21.2 Volumetrics- Solution-wise Requirements	12. Application Security Testing Tool	All the inline components of the solution must operate in high availability mode. In the event of any component failure, the system should automatically initiate failovers within seconds, ensuring uninterrupted functionality without requiring manual intervention.	Application Security Testing as a technology in general works at developemnt/pre-production/UAT stage only. And hence as a solution there is no need of high availability mode. Same has already been updated in this RFP (as solution is asked in standalone at both DC & DR). So, request bank to deleted this clause.	No Change, Please be guided by the RFP. The bidder must design the solution to fully comply with the RFP requirements, ensuring that in case of a failover, the system meets the defined SLA for availability, RTO, and RPO. The bidder is required to adhere to the deployment requirements outlined in the RFP when designing and proposing the solution architecture.
601	40	APPENDIX 1A Functional Compliance Sheet (Solutions)	Network Detection & Response (NDR)	Pt 8. Proposed solution should generate a root cause analysis, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets.It should provide a platform for easier investigation like visual graphical view and timeline of the attack and it should support tagging of MITRE tactics, techniques and procedures used by the attacker in alerts and incidents.	We reqeust bank to amend the clause: Proposed solution should generate a root cause analysis / incident management, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets.It should provide a platform for easier investigation like visual graphical view and timeline of the attack and it should support tagging of MITRE tactics, techniques and procedures used by the attacker in alerts and incidents.	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
602	40	APPENDIX 1A Functional Compliance Sheet (Solutions)	Network Detection & Response (NDR)	Pt 13. The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	As bank has asked for on-premise solution for NDR, on the contrary, this clause asks for cloud-native SAAS ask. So, we kindly request bank to delete this clause.	Please refer Addendum for revised clause
603	42	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 3. The solution must be able to analyse a wide array of programming languages including Java,.Net, C/C++, Objective-C, Android, PHP, COBOL, Ruby, Swift, HTML 5, Scala, APEX, TypeScript, Go, Kotlin and ABAP etc but not limited to these alone	Considering the future requirements of AI in Secure Code Development and most of the development is moving towards AI generated code using AI supported languages. So it is very important for bank to have coverage around this as well and will recommend to incorporate AI supported languages like "R, Ada, Solidity, Bash, Groovy, Rust, Perl", but not limited to these alone.	No Change, Please be guided by the RFP
604	42	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 24. Solution should support Machine learning and Analysis based on the archived results	ML capability is important, but it is very important to have coverage around AI based code as well. And will recommend bank to consider: The solution should have the capability to scan AI generated code. The solution should be able to integrate with AI coding agent via MCP	No Change, Please be guided by the RFP
605	43	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 32. The solution should be able to support Composition Analysis: Identify the opens source components used in the application. Vulnerabilities & outdated version Licensing risk associated with the components	Bank is looking for Software composition analysis and asked for identifying the open source component and licensing risk. But this limited information is not enough for bank to secure themselves with rapidly increasing supply chain attacks and we will highly recommend to consider following as well: SCA system must catalogue open source components from Maven, NPM, and Nuget. SCA system has to be able to generate a Bill of Materials for an application. Solution should have the ability to continuously monitor the scanned components & notify if there are any zero day attacks without performing the rescan. Solution should Catalog, Store, and Audit SBOMs (both cycloneDx & SPDX) generated for in-house developed software applications and COTS applications.	No Change, Please be guided by the RFP
606	30	7.2 Solution & Services Deployment Model and Their HA Requirement 7.2.1 Solutions – Master Deployment Matrix	Sl. No. 8	Vulnerability assessment (VA) & vulnerability lifecycle management Bank Location: Standalone at DC and Standalone at DR. Management Console: Deployed at both DC and DR	Requesting clarifications if standalone management console in DR will be live or will be on standby ?	Please refer addendum for revised clause
607	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 1 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall be deployable entirely on-premises and shall not require any cloud-hosted component, external service, or Internet connectivity for its core functionality, scanning, management, reporting, analytics, or product capabilities.	Requesting change to: The proposed solution shall be deployable entirely on-premises or hosted on MeitY cloud or Meity empanelled cloud environment. No data shall be shared with the platform/cloud outside India geolocation.	Please refer addendum for the revised clause
608	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 3 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall be software-based and fully deployable on the hardware infrastructure proposed by the Bidder.	Requesting change to: The proposed solution shall be software-based and fully deployable on the hardware infrastructure or should support hybrid- on-premise architecture with management-console or scanners on on-premise and analytics components on MeitY/MeitY-emapanneled cloud proposed by the Bidder.	No Change, Please be guided by the RFP
609	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 9 of Vulnerability Assessment & vulnerability lifecycle Management	Each scanning engine shall support web application security assessment together with traditional infrastructure vulnerability and configuration/compliance assessment. The solution shall identify vulnerabilities, missing patches, insecure configurations, and compliance deviations, and generate comprehensive reports containing risk severity, evidence of findings, affected assets, and remediation recommendations to support security governance, audit, and regulatory compliance.	Requesting to confirm that if DAST specs are specifically provided for web-application's VAPT, then what is the scope of "web-application" scanning in this spec? Also requesting to share the total number of web-applications considered in the scanning scope.	No Change, Please be guided by the RFP
610	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 18 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall support both active and passive asset discovery and vulnerability assessment/scanning.	Requesting change to: The proposed solution shall support both active and/or passive asset discovery and vulnerability assessment/scanning.	No Change, Please be guided by the RFP
611	48	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 27 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall support both active and passive techniques for vulnerability detection, where applicable.	Requesting change to: The proposed solution shall support both active and/or passive techniques for vulnerability detection, where applicable.	No Change, Please be guided by the RFP
612	48	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 33 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall support deployment and lifecycle management of scanning agents without dependency on cloud-hosted services.	Requesting change to: The proposed solution shall support deployment and lifecycle management of scanning agents.	No Change, Please be guided by the RFP
613	48	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 34 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall assess Active Directory security posture and identify misconfigurations, privilege risks, insecure policies, and exposure of critical directory services.	Requesting to clarify that this spec is already addressed in IDTR then what is the requirement of it in VM solutin?	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
614	49	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 74 of Vulnerability Assessment & vulnerability lifecycle Management	The solution shall support offline signature and plugin updates for deployment in isolated or air-gapped environments.	Requesitng to remove this spec because if the cloud-based solution is offered and where cloud is hosted on MeitY cloud or MeitY empanneled cloud then questions related to air-gap environment doesn't arise.	No Change, Please be guided by the RFP
615	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 81 of Vulnerability Assessment & vulnerability lifecycle Management	The solution shall support password-protected and/or digitally signed reports with configurable retention and archival.	Requesting change to: The solution must support secure, encrypted report distribution (including native PGP encryption) and enforce strict role-based access controls (RBAC) for report viewing. Additionally, the platform must provide configurable cloud-based data retention policies alongside automated options to archive historical scan data and reports to external storage	No Change, Please be guided by the RFP
616	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 87 of Vulnerability Assessment & vulnerability lifecycle Management	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	Requesting change to: The solution must provide AI-generated risk summaries and plain-language vulnerability briefs that automatically fuse asset criticality, technical findings, and real-world threat telemetry (such as CISA KEV and EPSS data) to streamline IT triage. If cloud analytics are utilized to run these machine learning models, the solution vendor must guarantee that all data is isolated within dedicated, bank-authorized cloud regions, employing strict data privacy frameworks that ensure source code, credentials, and raw scan parameters are explicitly excluded from public AI training models or multi-tenant public AI services	Please refer addendum for revised clause
617	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 88 of Vulnerability Assessment & vulnerability lifecycle Management	Unified, correlated findings intelligence. Every scanning engine — across web, API, network and host, cloud, containers, mobile, source code, device configuration and identity — reports into a single normalized findings model..	Requesting clarification on why unified reporting is asked as the ASM, VM, DAST solutions are considered separately.	No Change, Please be guided by the RFP
618	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 90 of Vulnerability Assessment & vulnerability lifecycle Management	Mobile Application Security Testing: The proposed solution shall support static security analysis of Android and iOS mobile application packages, including APK/AAB and IPA formats, and shall provide security assessment mapped to recognized mobile application security standards and methodologies such as OWASP MASVS and MASTG.	Requesting clarification for the spec as the ask is for DAST or MAST solution.	No Change, Please be guided by the RFP
619	87	Anti Phishing Services	17.1	Solution should detect at the earliest point in the attack, post initial compromise as the attacker is first attempting to move laterally and escalate privilege.	Since this section is focused on Anti-Phishing, we understand that the objective is to identify suspicious activity following a successful phishing or account-compromise event. Network-level lateral movement and deception capabilities may be addressed by other security controls. We request the Bank to clarify whether this clause may instead focus on early post-compromise user activity visibility for the Bank's most critical users. " The solution should support early identification and investigation of suspicious user activities associated with potential account compromise following phishing or other email-originated attacks, with enhanced user activity monitoring for up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles."	Please refer to the relevant Addendum for updated specfications
620	87	Anti Phishing Services	17.4	Solution must provide robust supply chain and AI/ML-driven contact chain analysis capabilities to identify and defend against socially engineered, impersonated, or BEC attacks.	As compromise of trusted suppliers and partners is an important source of BEC and phishing risk, we request the Bank to clarify whether the existing supply-chain requirement should explicitly include behavioural analysis of supplier/partner communication patterns to identify attacks originating from compromised trusted accounts. " Solution must provide robust supply-chain and AI/ML-driven contact-chain and behavioural analysis capabilities to identify and defend against socially engineered, impersonated or BEC attacks, including threats originating from compromised or impersonated supplier/partner accounts."	Please refer to the relevant Addendum for updated specfications
621	87	Anti Phishing Services	18	Solution must proactively analyze suspicious URLs using dynamic/behavioral analysis to prevent the spread of malware and other threats.	The RFP separately addresses URL analysis and post-delivery remediation. We request clarification whether these requirements are intended to provide continuous protection throughout the email threat lifecycle, including pre-delivery analysis, click-time URL protection and post-delivery detection/remediation. " Solution must provide continuous protection across the email threat lifecycle, including pre-delivery threat detection, real-time/click-time inspection of suspicious URLs, and post-delivery detection and automated remediation of threats that are subsequently determined to be malicious."	Please refer to the relevant Addendum for updated specfications
622	88	Anti Phishing Services	19.7	Solution must be able to offer a comprehensive portal that allows users to access information and metadata on events/incidents, facilitating network threat forensics for thorough investigation and analysis of potential security breaches or incidents.	To strengthen investigation of phishing-led incidents involving executives and other critical users, we request clarification whether the existing forensic portal requirement may also include contextual user and endpoint activity for a limited population of Bank-identified critical/high-risk users. " Solution must offer a comprehensive investigation portal providing information and metadata on events/incidents for forensic analysis. For up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, the portal should additionally provide contextual user and endpoint activity, including relevant application, file and user-action details, to support investigation of potential phishing-led compromise."	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
623	88	Anti Phishing Services	19.9	Solution must empower security operations and incident responders to automate the identification, remediation, and sharing of phishing threats, streamlining the process of detecting, addressing, and disseminating information about potential phishing attacks for improved response and mitigation.	To improve SOC investigation efficiency, we request clarification whether the existing phishing identification and remediation requirement should include centralized attack context showing why a message was identified as malicious, the users targeted, associated threat indicators and remediation status. " Solution must empower security operations and incident responders to automate identification, investigation, remediation and sharing of phishing threats, and should provide centralized contextual visibility into the users targeted, associated threat indicators, detection rationale, attack characteristics and remediation actions."	Please refer to the relevant Addendum for updated specfications
624	88	Anti Phishing Services	19.1	Solution must provide incident responders with real-time analytics and visibility into email-based attacks targeting the organization.	Email-based attacks against executives and privileged users may require additional context after delivery to determine whether a targeted user has subsequently performed suspicious activity. We request the Bank to clarify whether real-time investigation visibility may include relevant user activity context for up to 100 Bank-identified critical/high-risk users. " Solution must provide incident responders with real-time analytics and visibility into email-based attacks targeting the organization. For up to 100 Bank-identified critical/high-risk users, the solution should additionally provide contextual visibility into suspicious user activities associated with potential phishing or account compromise, including relevant user, endpoint, application and file activity."	Please refer to the relevant Addendum for updated specfications
625	88	Anti Phishing Services	19.23	Solution must have simplicity of evaluation and additional visibility into internal traffic and other communication channels can reduce risk, and baseline user activity to detect suspicious behavior.	The existing clause already seeks baselining of user activity to detect suspicious behaviour. We request the Bank to clarify the intended depth and scope of this capability and whether enhanced monitoring may be applied to a focused population of up to 100 Bank-identified critical/high-risk users, where deeper visibility provides the greatest security value. " Solution must provide additional visibility into relevant internal activity and communication channels to reduce risk and baseline user activity to detect suspicious behaviour. Enhanced user and data activity monitoring should be provided for up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, with configurable detection policies for suspicious, anomalous or policy-violating activities."	Please refer to the relevant Addendum for updated specfications
626	90	Anti Phishing Services	19.7	Solution must provide protection against harassment mail and mitigate the risks associated with emails from unknown senders specifically for executives or VIPs, safeguarding them from potential threats and ensuring their email communication remains secure.	Since this clause already provides enhanced protection for executives/VIPs, we request the Bank to clarify whether such enhanced protection should extend beyond receipt of suspicious email to investigation of risky user and data activities that may occur following phishing or account compromise, for a limited set of the Bank's most critical users. "Solution must provide protection against harassment mail and mitigate risks associated with emails from unknown senders specifically for executives or VIPs. For up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, the solution should additionally provide enhanced visibility into risky user and data activities following suspected phishing or account compromise, including relevant file movement, web/upload activity, removable-media activity and other supported data-transfer channels."	Please refer to the relevant Addendum for updated specfications
627	52	Idendity Threat Detection and Response (ITDR)	1.7	Detect and respond to active threats with high fidelity (low false positives and false negatives).	The Bank has separately specified a comprehensive deception platform for detection of active attacker activity, reconnaissance and lateral movement. We understand that the intent of this clause within ITDR is therefore to complement those controls with focused monitoring of the Bank's most critical identities. Considering that enhanced user-activity monitoring is most relevant for high-risk personnel such as executives, privileged users and other critical users, we request the Bank to kindly clarify whether this requirement may be read as follows: " Identity Threat Detection Solution should provide high-fidelity detection and response for risky or anomalous user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, to identify activities associated with careless, malicious or compromised users. "	No Change, Please be guided by the RFP
628	52	Idendity Threat Detection and Response (ITDR)	1.8	Provide contextual information—who, what, when and how—to inform all stages of the attack chain.	The Bank has already sought attack-lifecycle visibility under the separate deception requirements. For ITDR, we understand that additional value would be derived from detailed user-centric context for the Bank's most critical identities, enabling investigation of risky activity performed by such users. We request the Bank to kindly clarify whether this requirement may be read as follows: " Identity Threat Detection Solution should provide contextual information—who, what, when, where and how—around risky user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, to support investigation and response."	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
629	52	Idendity Threat Detection and Response (ITDR)	1.9	Provide deep insights into both the potential and used privilege escalation and lateral movement steps in an attack.	Privilege escalation and lateral-movement visibility is already substantially addressed under the separately specified deception solution, including attacker lifecycle visibility, MITRE ATT&CK mapping, deceptive attack paths and detection of lateral movement. To avoid duplication while retaining complementary investigation capability for high-risk identities, we request the Bank to kindly clarify whether this requirement may be read as follows: "Identity Threat Detection Solution should provide deep insights into activities performed by up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, covering application usage, file and data movement, endpoint activity and other risky behaviours to support investigation of compromised, malicious or negligent user activity."	No Change, Please be guided by the RFP
630	52	Idendity Threat Detection and Response (ITDR)	2.9	Detect all types of attack vectors including pre-attack reconnaissance, zero-day attacks, privilege escalation prevention, lateral movement and data theft.	Pre-attack reconnaissance, lateral movement, malware/attack behaviour and attacker lifecycle visibility are already covered under the Bank's separate deception specifications. We understand that the complementary requirement under ITDR should focus on identity/user risk and potential data-loss activity for the Bank's most critical users rather than duplicate the deception control. We request the Bank to kindly clarify whether this requirement may be read as follows: " Identity Threat Detection Solution should detect risky user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, including suspicious application usage, unauthorized access or movement of sensitive information, removable-media activity, web-based transfer, cloud synchronization and other potential data-exfiltration activities."	The Clause is applicable only to idendity related threat vector only. The volumetrics is provided in the RFP and should be complied
631	52	Idendity Threat Detection and Response (ITDR)	2.10	Detect multiple attacks simultaneously.	We understand the intent is to ensure that the solution is not restricted to investigation of a single event at a time. Since active attacker detection is separately covered by the deception solution, we request that this clause be clarified in terms of concurrent monitoring and investigation of risky activities across the Bank's designated critical-user population: "Identity Threat Detection Solution should be capable of detecting and investigating multiple risky user and data activities simultaneously across up to 100 critical/high-risk users and their monitored endpoints."	No Change, Please be guided by the RFP
632	52	Idendity Threat Detection and Response (ITDR)	3.2	Provide unified presentation of both source- and target-based telemetry data in a timeline view.	The Bank has separately specified end-to-end attacker visibility and behavioural analysis under the deception solution. For ITDR investigations involving critical identities, a chronological user-activity view would provide complementary evidence of actions performed by the user. We request the Bank to kindly clarify whether the requirement may be read as follows: " Identity Threat Detection Solution should provide a unified chronological timeline of user- and endpoint-based activity telemetry for up to 100 critical/high-risk users identified by the Bank to support investigation of risky or suspicious user activity."	No Change, Please be guided by the RFP
633	52	Idendity Threat Detection and Response (ITDR)	3.3	Correlate identity-related telemetry from relevant source and target systems to identify and investigate identity compromise, privilege escalation, credential abuse and lateral movement.	Privilege escalation and lateral-movement detection are already addressed through the separately specified deception controls. To provide complementary investigation capability for the Bank's highest-risk identities, we request the Bank to clarify whether this clause may focus on correlation of user, endpoint, application and data activity for the designated critical-user population: " The solution shall support correlation of user, endpoint, application and data-activity telemetry for up to 100 critical/high-risk users identified by the Bank to identify and investigate suspicious user behaviour, sensitive-data movement, policy violations and potential data-exfiltration activities."	No Change, Please be guided by the RFP
634	52	Idendity Threat Detection and Response (ITDR)	3.4	Integrate with compatible endpoint/extended detection solution to capture screen recordings or screenshots during active attacker sessions as advanced forensic evidence.	The Bank has separately specified attacker-session and forensic visibility through the deception platform. Within ITDR, we understand that visual evidence is intended to strengthen investigation of high-risk user activity. We request the Bank to kindly clarify whether the requirement may be read in an outcome-based manner for the designated critical-user population: " The Identity Threat Detection Solution should support screenshots, screen capture or equivalent visual evidence of relevant activity for up to 100 critical/high-risk users during suspicious or high-risk user sessions, as part of forensic investigation and evidence collection."	Please refer addendum for revised clause.
635	52	Idendity Threat Detection and Response (ITDR)	3.5	Integrate with compatible network detection solution to support collection of PCAP data for network-level incident visibility.	The requirement for PCAP is network-centric and does not directly relate to identity posture or focused user-activity monitoring. Further, the Bank's separate deception specifications already require high-interaction decoys, recording of attacker activities, traffic/behaviour visibility, forensic investigation and integration with network/security technologies. To avoid duplication of network-level forensic controls across two solution categories, we request the Bank to kindly delete this clause from the ITDR section.	Please refer addendum for revised clause.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
636	52	Idendity Threat Detection and Response (ITDR)	3.6	Push incident data into SIEM/XDR or SOAR technologies via integrations for improved incident management.	We understand that the objective is to ensure relevant ITDR alerts and investigation context are available to the Bank's SOC ecosystem. For the enhanced monitoring of designated critical users, we request the Bank to kindly clarify whether alerts and activity information may be shared through supported integrations or APIs as follows: " Identity Threat Detection Solution should make alerts and relevant incident/activity data for the monitored critical-user population available to SIEM/XDR, SOAR or other supported security platforms through integrations or APIs for improved incident management."	The proposed solution hould be integrated with SIEM/XDR or SOAR technologies for sharing the incident data via supported integrattion or APIs
637	52	Idendity Threat Detection and Response (ITDR)	3.7	As part of forensic data collection, include detailed attack path information including protocols leveraged during the attack.	Detailed attack-path and attacker-behaviour visibility is already sought under the separate deception specifications, including deceptive attack paths, MITRE ATT&CK mapping and forensic investigation. To avoid overlap while retaining complementary evidence for investigations involving the Bank's critical identities, we request the Bank to kindly clarify whether the requirement may be read as follows: " Identity Threat Detection Solution should, as part of forensic data collection for up to 100 critical/high-risk users, include detailed user-activity information such as applications used, files accessed, data movement, destination channels and other relevant endpoint activity associated with the incident."	Please refer addendum for revised clause
638	52	Idendity Threat Detection and Response (ITDR)	3.8	Collect user and computer information from Active Directory as part of forensic data gathering to enhance context and assess risk exposure.	We understand that directory information is required to enrich investigations with user and computer context. We request the Bank to clarify that enterprise identity context may be maintained for the overall identity population, while detailed endpoint/user-activity telemetry may be applied to the Bank's designated critical-user population: " Identity Threat Detection Solution should use relevant user and computer identity information to enhance forensic context and risk assessment, and should correlate such context with detailed endpoint/user-activity telemetry for up to 100 critical/high-risk users identified by the Bank."	Please refer addendum for revised clause
639	52	Idendity Threat Detection and Response (ITDR)	3.9	Detect an adversary's attempt to move laterally toward key assets using as many Windows, Mac or Linux hosts as possible without requiring a persistent agent.	The Bank's separate deception specifications expressly require detection of lateral movement, reconnaissance, credential theft and malicious activity using agentless and/or agent-based deception techniques across the enterprise. The present clause therefore duplicates a capability already being procured under the Deception section. To avoid overlapping scope and duplicate controls, we request the Bank to kindly delete this clause from the ITDR section.	Please refer addendum for revised clause
640	52	Idendity Threat Detection and Response (ITDR)	3.10	Collect AD user/computer information for forensic context and detect at the earliest point post initial compromise as the attacker first attempts lateral movement and privilege escalation.	Early detection of lateral movement and privilege-escalation activity is substantially covered under the Bank's separate deception requirements. To retain a complementary identity/user-risk objective without duplicating the deception scope, we request the Bank to kindly clarify whether this clause may focus on early detection of risky activity among the designated critical-user population: " Identity Threat Detection Solution should use relevant identity context and detect risky user behaviour at the earliest possible point for up to 100 critical/high-risk users, based on monitored endpoint activities and configured detection policies, enabling investigation and response before such activity results in significant data loss or business impact."	Please refer addendum for revised clause
641	52	Idendity Threat Detection and Response (ITDR)	3.11	Collect AD user/computer data during forensic gathering while ensuring all deception techniques remain hidden from legitimate users.	The requirement to ensure deception techniques remain hidden from legitimate users is inherently a deception-platform capability. The Bank has already included comprehensive deception requirements covering lures, breadcrumbs, fake credentials, deceptive assets, attacker engagement and techniques designed to remain undetected by attackers. We therefore request the Bank to kindly delete this clause from the ITDR section to avoid duplication.	Please refer addendum for revised clause.
642	2	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	10	OEM shall ensure compliance of the complete proposed solution & platform with RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and all applicable regulations throughout the contract period.	We request the Bank to clarify that the OEM is required to maintain applicable security, privacy and regulatory controls relevant to the services provided and furnish available compliance/assurance documentation, while the overall regulatory compliance obligation of the Bank remains subject to the Bank's deployment, configuration and usage of the service. " OEM shall maintain security, privacy and compliance controls applicable to the proposed hosted service and shall provide available independent assurance reports, certifications and relevant compliance documentation to support the Bank's obligations under applicable RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and other applicable regulatory requirements."	Please refer addendum for revised clause
643	2	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	20	The Service uptime agreement for the proposed solution on cloud should have monthly uptime commitments and have transparent monthly credit calculations in case of uptime not being met for any services.	We understand that published/contracted OEM hosted-service SLA commitments and corresponding service-credit methodology shall meet this requirement. Kindly confirm.	No Change, Please be guided by the RFP
644	3	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	29	Solution provider should provide the design and process for data deletion in the scope of an independent audit and that the operational effectiveness of these controls is tested. The report for the same should be submitted to bank as and when asked by bank.	For a globally operated hosted security service, control effectiveness is generally evidenced through independent assurance reports such as SOC 2 Type II and documented data-retention/deletion controls. We request the Bank to permit such independent assurance documentation instead of requiring a separate bespoke data-deletion audit report. " Solution provider shall maintain documented secure data-retention and deletion controls. Compliance may be demonstrated through applicable independent third-party assurance reports/certifications (such as SOC 2 Type II or equivalent) and documented data-retention/deletion policies made available subject to OEM confidentiality requirements."	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
645	4	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	41.3	Independent audit for testing effectiveness of secure data removal, such that data is rendered permanently inaccessible. (Including any backup or distributed online media).	We request the Bank to accept independently audited secure deletion and media-management controls, together with documented retention/deletion periods, rather than requiring a customer-specific audit of all backup and distributed media. " The OEM shall maintain secure data deletion, media handling and backup-retention controls designed to render customer data inaccessible in accordance with documented retention schedules. Effectiveness may be evidenced through independent assurance reports such as SOC 2 Type II/ISO 27001 or equivalent and relevant OEM security/privacy documentation."	Please refer addendum for the revised clause
646	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	47.2	Bank shall have an option to implement 'Bring Your Own Key' as and when required.	The proposed service protects data at rest and in transit using strong encryption; however, customer-managed infrastructure encryption keys are not a standard capability of the hosted anti phishing service. We request deletion of the BYOK requirement, or acceptance of OEM-managed enterprise-grade encryption and key-management controls. " Requested Action: Delete the BYOK requirement. Alternatively: 'Data processed/stored by the hosted service shall be protected using industry-standard encryption in transit and at rest, with secure OEM-managed key-management controls subject to independent security assurance.'"	Please refer addendum for the revised clause
647	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	49	Web Application Firewall shall be implemented on the cloud for Web based applications. WAF application signature should be updated and reviewed regularly. The Report shall be submitted to bank on a periodic interval.	Since the proposed platform is an OEM-managed hosted security service, underlying WAF technology, signatures and configurations form part of the OEM's internal security architecture and may not be exposed as customer-specific reports. We request the Bank to accept periodic VAPT/penetration-test assurance or equivalent independent security assessment evidence covering the hosted application instead of WAF signature reports. " The hosted web application/platform shall be protected through appropriate application-security controls. The OEM shall conduct periodic vulnerability assessment and penetration testing/security assessments and, subject to confidentiality restrictions, provide an executive summary/attestation or applicable independent assurance evidence to the Bank on request. Customer-specific WAF signature reports shall not be mandatory."	Please refer addendum for revised clause
648	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	52	The systems in cloud infrastructure should be periodically updated with the latest anti-malware signatures, the bidder shall submit the periodic report on the same with bank.	For an OEM-managed hosted security service, infrastructure anti-malware/endpoint controls are centrally managed and independently audited. We request the Bank to accept OEM security assurance and vulnerability/malware-control attestations rather than periodic host-level signature reports. " The OEM shall maintain appropriate malware protection, vulnerability management, patching and security monitoring controls for the hosted infrastructure. Compliance may be evidenced through independent assurance reports/certifications and applicable security-control attestations instead of customer-specific anti-malware signature update reports."	Please refer addendum for revised clause
649	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	53	Data Loss Governance and risk management framework shall be defined by bidder for workload on the cloud and same shall be shared with bank on periodic basis. Data loss prevention controls should be implemented to secure the data in the cloud environment from unauthorized or inadvertent exfiltration.	We request clarification that the requirement is intended to ensure protection against unauthorized/inadvertent data exfiltration through the proposed service and appropriate security controls for hosted customer data, rather than requiring disclosure of the OEM's internal cloud governance framework. " The proposed solution shall provide configurable controls to identify and prevent unauthorized or inadvertent transmission/exfiltration of sensitive information through any channels. The OEM shall maintain appropriate access control, encryption and data-protection controls for customer data processed within the hosted service and provide applicable assurance documentation on request."	Please refer addendum for revised clause
650	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	81	Log generation, storage and review process should be certified by CERT IN empaneled auditor, report for the same shall be submitted by bidder as and when required by bank.	For global SaaS/POD services, security logging and monitoring controls are typically independently audited under recognized assurance frameworks. We request the Bank to accept SOC 2 Type II/ISO 27001 or equivalent independent assurance in lieu of a mandatory CERT-In-empanelled audit of the OEM's internal log-generation/storage/review process. " The OEM shall maintain documented security logging, monitoring, retention and review controls. Effectiveness shall be evidenced through applicable independent third-party assurance reports/certifications such as SOC 2 Type II, ISO 27001 or equivalent. CERT-In-empanelled audit may be required only for bidder-managed components deployed specifically within the Bank environment, where applicable."	Please refer addendum for the revised clause
651	7		82.5	IT Act 2000 & its amendments, and other Acts/Regulatory guidelines. All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	Kindly clarify that the OEM must comply with legal/regulatory requirements applicable to it as the provider of the proposed hosted service and provide reasonable documentation to support the Bank's compliance obligations. " OEM shall comply with applicable legal and regulatory obligations relevant to its provision of the proposed service and shall provide available security/privacy/compliance documentation reasonably required to support the Bank's applicable obligations."	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
652	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	83	CERT IN Empaneled auditor report's is required for the following:	We request the Bank to permit internationally recognized independent assurance reports/certifications for OEM-managed hosted services. CERT-In empanelled audit reports may remain applicable to India-specific bidder-managed/on-premises components where such audit is feasible and required. " For OEM-managed hosted/SaaS services, independent assurance reports/certifications such as SOC 2 Type II, ISO 27001 or equivalent shall be accepted. CERT-In empanelled audit reports shall be applicable only to components/services for which such India-specific audit is contractually and technically feasible."	Please refer addendum for the revised clause
653	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	92	The application and DB is/will be hosted separately on a dedicated infrastructure (physical/logical) for PSB. Evidence of dedicated infrastructure (physical/logical) for PSB should be submitted.	The proposed platform is an OEM-managed hosted security service designed with logical access controls and customer data isolation. Requiring dedicated physical application/database infrastructure would restrict standard SaaS/POD architectures without necessarily improving the security outcome. We request acceptance of secure logical tenant/customer isolation supported by independent assurance evidence. " The proposed hosted service shall provide secure logical segregation/isolation of Bank data and administrative access from other customers through appropriate access-control and tenant-isolation mechanisms. Dedicated physical application/database infrastructure shall not be mandatory where equivalent logical isolation is implemented and independently assured."	Please refer addendum for the revised clause
654	8	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	98.1	Feasibility to audit/review IT controls of the third party or obtaining independent review report for the same from CERT-In empaneled security consultant, to ensure it meets Bank's information security requirement.	We request that the Bank permit review of current independent assurance reports/certifications as the primary mechanism for reviewing OEM IT controls. Any direct audit should remain subject to the OEM's standard contractual audit provisions, confidentiality, security, scope and advance-notice requirements." The Bank may review applicable independent third-party assurance reports/certifications covering the hosted service. Where additional audit is required, such audit shall be subject to mutually agreed scope, confidentiality/security restrictions, reasonable advance notice and the OEM's standard contractual audit provisions. A CERT-In empanelled consultant may review evidence made available under these conditions."	Please refer addendum for the revised clause
655	Appendix 1A Page 40	NDR Functional Compliance Sheet	Clause 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high- availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	The Clause mandates Cloud based SaaS model, while RFP Page 30, Page 35, section 7.2.4.1 clause 'd' asks for on Premesis solution "The NDR shall be deployed On-Premises". We request to modify the clause to include On-Prem solution. Justification: To include solutions which are on-Prem based	Please refer Addendum for revised clause
656	Appendix 1A Page 40	NDR Functional Compliance Sheet	Clause 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high- availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	The Clause asks for Active-Active HA architecture, we request to include Active-Standby Mode. Justification: Management Console is central console, it cannot be deployed in Active-Active mode, as it is a central component.	Please refer Addendum for revised clause
657	Appendix 1A Page 41	NDR Functional Compliance Sheet	Clause 18	Solution should have the capabilities to create and run security playbooks for automation and better MTTD/MTTR on the basis of criticality of threat/server	Proposed solution adopts below appraoch for automated MTTD, Solution need investigative workflows and all the alerts need to be validated before building any Active Response Solution is having inbuilt playbooks like Host, Session and Packet analysis. once alert is validated Active Response can be triggered. **Hope the approach is acceptable**	Yes, your understanding is correct Also, Please refer addendum for the revised clause
658	Page 66	7.6.7	Training	At a minimum, the following training programs shall be conducted for each proposed solution / OEM appointed officials: Duration per Session and Munimum Number of Sessions	Overall there is a requirement of 15 Sessions and Duration per session is 2 or 3 days. This takes the total training per solution to 40 days. This is very large reqirement of training, we request to make it to 3 days for NDR solution	Please refer addendum for revised clause
659	Page 63	7.6.6	Testing, clause 3	The bidder shall provision and maintain dedicated Development, Testing, UAT, and Pre-Production environments throughout the contract period.	Is UAT Environment required for NDR solution also, given that NDR is a Passive and out of path solution.	Please refer addendum for revised clause
660	30, 34	7.2.1 Deployment Model & HA (TIP) / 7.2.4.1 Deployment Pattern	Table 7.2.1 Sr. 7; Cl. 7.2.4.1(e)	"Threat Intelligence Platform (TIP) - Cloud (SaaS) + Hybrid - Bank Location: Broker/Collector/Integrator: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR" (Table 7.2.1).	Cyble's Threat Intelligence Platform (TIP) is delivered as a fully cloud-native SaaS solution, providing continuous threat-intelligence aggregation, enrichment and distribution to the Bank via API, STIX/TAXII feed and a dedicated web portal, with high availability, geographic resiliency and disaster recovery built into the SaaS platform itself - fully aligned with the SLA, RTO and RPO defined in Section 13. As the TIP's core function requires no packet-level or in-line processing within the Bank's network, Cyble can meet the Bank's continuity requirement for this solution without deploying a broker/collector component on Bank premises. We request the Bank's confirmation that this cloud-native delivery model will be accepted as fully compliant with Table 7.2.1.	Please refer addendum for the revised deployment requirement

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
661	31, 35	7.2.1 Deployment Model & HA (CSPM) / 7.2.4.1 Deployment Pattern	Table 7.2.1 Sr. 11; Cl. 7.2.4.1(i)	"Cloud Security Posture Management (CSPM) - Cloud (SaaS) + Hybrid - Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR" (Table 7.2.1); "...with the required connectors, collectors, agents, enforcers and/or other supporting Bank-side components, if required, deployed at the Bank's DC and DR in N+N Active-Active configuration" (Cl. 7.2.4.1(i)).	Cyble's Cloud Security Posture Management (CSPM) module continuously assesses the Bank's cloud environments through secure, read-only, API-based/cross-account IAM-role integration, with no agent, connector or collector required on Bank premises. This lets Cyble deliver continuous, real-time cloud security posture monitoring with high availability and resilience built natively into the SaaS platform, fully meeting the Bank's SLA, RTO and RPO requirements under Section 13. This is consistent with the qualifying language "if required" already present in Cl. 7.2.4.1(i). We request the Bank's confirmation that this API-integrated, cloud-native delivery model will be accepted as compliant.	Please refer addendum for the revised clause
662	55-56	7.4.3 Attack Surface Management	Cl. 7.4.3	"Discovery of internet-facing and internal assets... The proposed solution shall provide AI-enabled Attack Surface Management (ASM) capabilities for continuous discovery... of the organization's external attack surface, including known and unknown internet-facing assets."	Cyble's Attack Surface Management (ASM) capability provides continuous, AI-enabled discovery, monitoring and risk-prioritization of the Bank's entire external attack surface - internet-facing assets, exposed services, domains, cloud assets and shadow IT - using external/passive reconnaissance together with Bank-shared asset inventories (IP ranges, domains, cloud accounts), with no agent or appliance required inside the Bank's network, consistent with the offsite Managed Service model in Section 7.2.2. This gives the Bank a complete outside-in exposure view from Day 1. We request the Bank's confirmation that this externally-led, agentless approach satisfies Cl. 7.4.3.	Bank is looking for external attack surface management
663	55	7.4.5 Anti-Phishing	Cl. 7.4.5	"...offsite continuous anti-phishing monitoring and response services for detection, analysis for phishing attacks targeting the Bank, its employees, customers, executives, digital assets, domains, and online channels."	Cyble is fully equipped to deliver continuous, 24x7 Anti-Phishing monitoring across the Bank's domains, executives and digital channels from Day 1 of the engagement, scaling seamlessly as the Bank's digital footprint grows, with no additional infrastructure required from the Bank. To finalise the onboarding plan, we request the Bank share the number of primary/registered domains, sub-domains, executive/VIP identities and customer-facing digital channels to be covered at contract commencement, so Cyble can confirm precise sizing against this scope.	Please refer to the relevant Addendum for updated specfications
664	57	7.4.6 Dark Web Monitoring	Cl. 7.4.6	"...offsite, tool-based continuous dark web and cyber threat exposure monitoring services... across the surface web, deep web, dark web, underground forums, messaging platforms, and data leak repositories."	Cyble's Dark Web & Cybercrime Monitoring capability continuously covers the surface web, deep web, dark web, underground forums, messaging platforms and data-leak repositories, and can begin protecting the Bank's specified identities, brand keywords and domains immediately upon contract signature. To tailor this coverage precisely, we request the Bank share the initial monitoring scope (employee/executive identities, brand keywords, domains and relevant data categories) so Cyble can confirm sizing and reporting cadence.	Details shall be shared with succesful bidder
665	57	7.4.7 Threat Intelligence Feed	Cl. 7.4.7(l)	"Provision of threat intelligence through a centralized portal/dashboard and/or machine-readable feeds."	Cyble's Threat Intelligence Feed is delivered through both a centralized portal/dashboard and machine-readable, standards-based feeds (STIX/TAXII, MISP-compatible formats and API), enabling seamless integration with the Bank's existing or future security stack whenever required. We confirm this dual delivery model - portal-based consumption plus machine-readable feed/API - and request the Bank's confirmation that it satisfies Cl. 7.4.7.	No Change, Please be guided by the RFP
666	57-58	7.4.8 Threat Hunting Services	Cl. 7.4.8(m)	"The threat hunting service shall be delivered remotely/offsite using secure and mutually agreed mechanisms for accessing relevant logs, telemetry, security tools, and data made available by the Bank."	Cyble can deliver proactive, intelligence-driven Threat Hunting entirely offsite - correlating curated external threat intelligence (IOCs, IOAs, TTPs, threat-actor and campaign intelligence) against Bank-shared context, supplemented by secure, mutually agreed read-only access to relevant Bank telemetry for validation and deeper investigation as needed - fully consistent with the remote/offsite delivery model mandated in Cl. 7.4.8(m). We request the Bank's confirmation that this intelligence-led hunting model, combined with agreed read-only telemetry access, meets the Bank's requirement.	No Change, Please be guided by the RFP
667	58	7.4.9 Brand Protection and Monitoring	Cl. 7.4.9(j)	"Takedown coordination with relevant registrars, hosting providers, platforms, application stores, social media platforms, and other relevant entities, wherever applicable."	Cyble's Brand Reputation Monitoring capability continuously identifies brand impersonation, typosquatting, phishing/fraudulent websites, fraudulent mobile apps and social-media impersonation, and actively coordinates takedown requests with registrars, hosting providers, app stores and social platforms on the Bank's behalf under a standard authorisation executed at contract signature - delivering a fully managed, end-to-end takedown process with minimal effort required from the Bank's team. We request the Bank's confirmation that this bidder-led takedown coordination model satisfies Cl. 7.4.9(j).	Please refer addendum for revised clause
668	256	16.21 Annexure 21: Sizing/Volumetrics (gap for Offsite Services)	Annexure 21, Sizing table	Annexure 21's sizing table provides explicit volumetrics (EPS, endpoint counts, IPs, VPCs, etc.) for the 14 solutions under Section 7.3, but no equivalent executive/VIP count is specified for the offsite services that monitor executive exposure (Anti-Phishing - Cl. 7.4.5, Dark Web Monitoring - Cl. 7.4.6, Brand Protection - Cl. 7.4.9).	Cyble's Executive Monitoring and Digital Risk Protection capabilities can protect any number of the Bank's executives/VIPs from Day 1, with coverage scaled precisely to the Bank's requirement across Anti-Phishing, Dark Web Monitoring and Brand Protection. To finalise sizing, we request the Bank confirm the number of executives/VIPs (e.g., Board members, CXOs, senior management) to be brought under continuous monitoring at contract commencement.	Please refer to the relevant Addendum for updated specfications
669	256	16.21 Annexure 21: Sizing/Volumetrics (gap for Offsite Services)	Annexure 21, Sizing table	As above - no domain/sub-domain count is specified for the offsite services that monitor the Bank's external digital footprint (Attack Surface Management - Cl. 7.4.3, Anti-Phishing - Cl. 7.4.5, Brand Protection - Cl. 7.4.9).	Cyble can bring any number of the Bank's domains and sub-domains under continuous monitoring across Attack Surface Management, Anti-Phishing and Brand Protection from Day 1. To finalise sizing, we request the Bank confirm the number of primary domains and sub-domains to be monitored at contract commencement, and the expected annual growth in this count.	details shall be shared with successful bidder

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
670	54	7.4 Functional Requirement - Services (Offsite Services)	Cl. 7.4(d)	"The Bidder shall implement appropriate security controls, including data masking or tokenization for sensitive data, Role-Based Access Control (RBAC), Just-in-Time (JIT) privileged access, and comprehensive audit logging for all services delivered under this RFP." - no named-user/license count is specified for platform/dashboard access to the 9 offsite services.	Cyble's platform can be provisioned for any number of the Bank's analysts, CISO-office and compliance stakeholders who need dashboard access to the offsite services, with full role-based access control as required under Cl. 7.4(d). To size the commercial bid precisely, we request the Bank confirm the number of named analyst/console user licenses required for the Bank's teams to access Cyble's platform and reporting for the proposed offsite services.	details shall be shared with successful bidder
671	55, 58	7.4.5 Anti-Phishing / 7.4.9 Brand Protection and Monitoring	Cl. 7.4.5; Cl. 7.4.9(j)	Neither clause, nor Annexure 21, specifies an expected volume of takedown actions per month/year for phishing sites, fraudulent domains, or fake social media/mobile app listings.	Cyble is fully equipped to execute takedown actions at whatever volume the Bank's threat exposure requires. To align commercial terms precisely with the Bank's risk profile, we request the Bank confirm the estimated number of takedown actions (phishing sites, fraudulent domains, fake social media/mobile app listings) expected per month under Anti-Phishing and Brand Protection.	Please refer to the relevant Addendum for updated specfications
672	98-99	9 PROJECT TIMELINES	Overall Implementation Period	9 PROJECT TIMELINES Overall Implementation period shall be 5 Months (Start Date is T0) for all solution & services The bidder shall submit a comprehensive Project Plan, within 7 days of T0 covering each proposed product/solution & Services, detailing all project phases, milestones, tasks, sub-tasks, activities, timelines, dependencies. The bidder shall submit the detailed Project Plan along with the proposal (mandatory) and subsequently within seven (7) days from T0 for the Bank's review and approval. Any Liquidated Damages (LD) for delays in project execution shall be calculated based on the bank's approved Project Plan.	Bidder requests confirmation that delays attributable to Bank dependencies, access, approvals, third-party vendors, connectivity, data availability or OEM/CSP dependencies will result in corresponding extension of timelines/relief from LDs.	No Change, Please be guided by the RFP
673	98-99	9 PROJECT TIMELINES	Project Plan	9 PROJECT TIMELINES Overall Implementation period shall be 5 Months (Start Date is T0) for all solution & services The bidder shall submit a comprehensive Project Plan, within 7 days of T0 covering each proposed product/solution & Services, detailing all project phases, milestones, tasks, sub-tasks, activities, timelines, dependencies. The bidder shall submit the detailed Project Plan along with the proposal (mandatory) and subsequently within seven (7) days from T0 for the Bank's review and approval. Any Liquidated Damages (LD) for delays in project execution shall be calculated based on the bank's approved Project Plan.	Please confirm that the bidder's submitted project plan, once reviewed and mutually agreed with the Bank, will form the baseline, and that changes arising from Bank-side dependencies or scope changes will be incorporated through a documented change-control process.	No Change, Please be guided by the RFP
674	98	8 CONTRACT PERIOD	Contract Period	8 CONTRACT PERIOD The terms and conditions of purchase order and RFP (read with addendums/Corrigendum/ Clarifications) shall constitute a binding contract. The Bidder is required to sign the contract within 15 days from the date of acceptance of the Purchase Order. The contract period for the project is the Implementation Period (as mentioned in Section 9: Project Timelines) + Support period (60 Month Post Go-live) which will commence from the effective date of agreement. The bank may, at its sole discretion, extend the contract for an additional period of two years, in one-year increments tranches. The Bank may extend the support services for an additional period of up to two (2) years beyond the original contract period. The pricing applicable during the extension period shall be mutually agreed and shall not exceed 120% of last year's AMC/ATS/Facility management rates quoted by the Selected Bidder. The decision to further extend the contract with the same bidder shall be at the sole discretion of the Bank. Further, the Bank will have the right to renegotiate prices of AMC, ATS, Facility Management rates at the end of the contract period. End of Sales / End of support: The bidder must ensure that any equipment (hardware/software) supplied as part of this RFP	Please confirm that the base contract term is 5 months implementation + 60 months O&M/support, and that the optional two-year extension will be on mutually agreed/quoted rates rather than being deemed included in the base TCO. Please also clarify the pricing mechanism applicable during the extension period.	No Change, Please be guided by the RFP
675	93	7.19.1 Other Scope Activity	OEM Discontinuation/Change of Control Pre-Award	7.19.1 Other Scope Activity (item 4): Respective solution OEM along with the bidder must note that it shall not be permitted to change the proposed OEM Solution after submission of bid. Bidder must also note that it shall not be permitted to quote any options of solution/OEM. Failure to adhere to this clause may attract disqualification of the bid/contract as well as invoke related damage clauses.	Please clarify the process, if any, for a bidder to seek Bank approval for OEM/product substitution in the limited event that the originally proposed OEM entity is acquired, ceases business operations, or formally discontinues (End-of-Sale/End-of-Life) the proposed product during the project's full duration, for reasons entirely outside the bidder's control.	Pleae be guided by the RFP
676	93	7.19.1 Other Scope Activity	Regulatory Change Scope - Existing vs New Functionality	7.19.1 Other Scope Activity (item 2): Statutory and regulatory changes...mandating change/s to an existing functionality of the Solution shall be provided to the Bank at no additional cost for the entire contract period. However, any Statutory and Regulatory changes post Go-Live of the respective applications (which are not a part of the existing functionalities) will be on CR basis based on the rates provided in the Bill of Material.	Kindly confirm that the this clause is applicable only for the period between bid submission and award of contract.	The requirement applies throughout the entire contract period as stated in the RFP.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
677	93	7.19.1 Other Scope Activity	UI/UX Customization Scope Boundary	7.19.1 Other Scope Activity (items 5-6): The Respective Solution OEM along with the bidder is expected to customize the screens, design and layout of the solution depending on the requirements of the bank, at no additional cost to the bank as per the specific UI/UX design finalized during the SRS. The Respective solution OEM along with the bidder is expected to customize the solution based on the requirements of bank.	Please confirm that no-cost UI/UX and solution customization is limited to configuration within each OEM product's standard/native customization framework, and that customization requiring source-code-level development, new modules, or capabilities outside the product's native framework will be handled through the change-control process at commercial rates.	The bidder shall submit sizing assumptions, bandwidth calculations, latency requirements and redundancy architecture.
678	89-92	7.18 IT Infrastructure	Infrastructure Sizing	7.18 IT Infrastructure requirements 1. Bidders must design, size, supply, commission, maintain and manage suitable and required hardware infrastructure for the proposed solutions in the RFP response at the location specified in the RFP (DC and DR). Bidder should size hardware based on the volumes mentioned in Annexure 21: Volumetrics of this RFP at relevant locations- DC, DRC and branches. 2. If the proposed solution is cloud-based, the bidder must accurately right-size the cloud infrastructure to meet all performance, capacity, and SLA requirements outlined in the RFP. The design should ensure availability within the primary cloud site, incorporating failovers, backups, and health monitoring, while also including a disaster recovery plan with a secondary site that meets the defined requirement as stated in the RFP. The proposal should include detailed architecture diagrams and a sizing justification. 3. The proposed hardware infrastructure should be of the latest production available infrastructure not older than 2025. 4. The proposed architecture shall ensure appropriate availability and failover within the primary cloud environment, applicable backup and health-monitoring capabilities, and disaster recovery through the required secondary site/DR architecture	Please clarify that additional capacity at no cost will apply only where the deficiency is attributable to incorrect bidder sizing against the RFP-provided baseline, and not where additional requirements arise due to new scope, material volume growth beyond stated volumetrics, Bank-initiated changes or third-party changes.	The bidder is responsible for correct/right sizing against the RFP requirements, stated volumetrics, retention, performance, SLA and reasonably foreseeable requirements expressly included in the RFP.
679	89	7.18 IT Infrastructure	Latest Production Hardware	The proposed hardware infrastructure should be of the latest production available technology and should not be older than 2025 as on the date of supply.	Please clarify whether 'not older than 2025' refers to manufacturing year of the physical equipment, model launch/availability date, or production/GA date. Also confirm whether current-generation hardware released after 2025 will be acceptable.	Please refer addendum for revised clause.
680	89	7.18 IT Infrastructure	Non-Production Environment	Bidder shall also provide a non-production environment for all proposed solutions as applicable, including necessary hardware/software/cloud resources and licenses, as part of the solution and at no additional cost to the Bank.	Please clarify the expected sizing/volumetrics for the non-production environment and whether logical/virtual separation is acceptable for cloud/SaaS components.	details shall be shared with successful bidder
681	88	7.17 System Recovery	Batch Job Restart Applicability to Cloud/SaaS Components	7.17 System recovery (item 7): The Bidder shall ensure that each batch job (if any) can, following a failure, be restarted from the point of failure once the cause of the failure has been removed.	Please confirm whether this batch-job restart-from-point-of-failure requirement applies only to Bank-hosted/on-premises components, or also to Cloud/SaaS-hosted solution components where the underlying batch/processing infrastructure is owned and controlled by the OEM/CSP.	The requirement applies to all components where batch processing/jobs are part of the proposed service. For SaaS components, the bidder/OEM shall provide equivalent recovery capability within the purview of the proposed solution/services and demonstrate compliance with the applicable operational requirements
682	84-88	7.15-7.17 / Services	Managed Security Services	7.15 NextGEN SOC operations: Bidder is responsible for below operational matters during the Contract period. 1. The bidder should manage, monitor, maintain and upgrade all NextGEN SOC solutions on ongoing basis encompassing all deployed hardware / firmware / middleware / software components by performing timely backups, continuous health monitoring, on- site and offsite support, troubleshooting, critical functional and performance bug fixes, all major product/feature enhancements within the warranty and AMC/ATS charges and as per the SLA defined by the Bank for Contract period. 2. All onsite resources should ensure to deliver the services leveraging NextGEN SOC technologies as mentioned in the technology details, architecture and Terms & conditions in the RFP, addendums, corrigendum, clarifications etc. issued by the Bank. 3. The onsite resources must be provided with adequate guidance, assistance & support by competent offsite subject matter experts (SME) of the bidder & OEMs. 4. Bidder to ensure efficient utilization and monitoring of Licenses, optimizing capacity utilization, ensuring quality of data and system performance is maintained optimal, there are no security events omission, misfiring rules, heavy rules and reports etc. 5. Participate and contribute to	Bidder proposes that a single integrated service-management platoform across all managed services components be evaluated, with common case IDs, evidence, severity, ownership and SLA reporting rather than disconnected OEM portals.	No Change, Please be guided by the RFP
683	83, 88	7.14 DR Drill / 7.17 System Recovery	DR Drill Frequency and Cost	7.14 DR Drill: The bidder is responsible for conducting the DR Drill on a regular basis and as per the frequency decided by the bank... 7.17 System recovery (item 2): Bidder to ensure that scheduled/unscheduled DR drills is conducted on regular basis (Quarterly basis or as defined by BANK).	Please confirm the baseline for DR drill frequency.	The minimum baseline shall be quarterly, unless a higher frequency is prescribed by the Bank, regulator, applicable standard or solution-specific requirement. The Bank may require additional drills where operational/security circumstances warrant.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
684	80-81	7.13 / Regulatory	Regulatory Evidence	upgrade the hardware, software, applications etc. to meet the Bank's expectations at no extra cost to the Bank. 45. Bidder should ensure the proposed technologies, services are capable & configurable to send logs, data, network traffic, security alerts etc. on demand to regulators like CSITE, CERT-in, NCIIPC etc. 46. If any hardware, software, application, services has got additional component, feature, functionality, load bearing capability, domestic & foreign compliance requirements, security arrangement etc. which can be activated / provided in the proposed setup just by activating licenses and without procuring any hardware, then the same should be activated and provided in the proposed setup of the Bank without any extra cost to the bank.	Bidder requests to understanding of the regulatory/audit evidence export mechanism that can preserve context, integrity, timestamps and chain of custody without weakening Bank security controls.	No Change, Please be guided by the RFP
685	78-80	7.13 / Logging	Log Baseline	6. Every technology deployed should transform itself from a purely rule based system to analytics & AI/ML based correlation system for logs, vulnerabilities & threat intelligence together for accurate risks prediction. 7. To ensure efficient utilization and monitoring of proposed solution, optimizing capacity utilization, ensuring quality of data and system performance is maintained optimal, there are no security events omission, misfiring rules, heavy rules and reports etc. 8. Participate and contribute in every DR drill, cyber security drill, tabletop exercises by the Bank, regulators or any third party. 9. Conduct DR drill of the Security on quarterly interval or as and when required by the Bank. Ensure DC & DR are exact replica of each other in every manner. 10. Develop custom plug-ins, parsers, connectors, agents, adopters for all the systems in the Bank or related to the Bank periodically or as and when needed. 11. Develop the baseline for the level of logs to be enabled across the different components of IT including infrastructure, databases, business applications and devices etc. The log baselines should be in line with global best practices including NIST, SANS etc. 12. Perform monthly gap analysis of current levels of logs enabled in OS, databases, web servers, business applications and devices and entire	Bidder requests for an initial application/infrastructure logging baseline and a monthly coverage score showing enabled sources, expected events, observed events, parser health and gaps by criticality.	The Bank shall provide the available details of the existing application/infrastructure logging environment and relevant log sources, to the extent available, during the implementation/onboarding phase.
686	78-80	7.13 / Resilience	Configuration Backup	17. Define formats for MIS reporting that includes daily, weekly and monthly or any periodical or adhoc reports, dashboards as per the Bank's requirements. 18. Devise rules, AI/ML based models to analyse logs received from business applications to alert application owners about potential security threat / incident. OWASP and other threat modelling must be used for creating such rules, models. A minimum 15 unique use cases should be developed and implemented for each business application within first six months of go live date. 19. Transfer the knowledge to the Bank's employees about day-to-day operations, system / backend level troubleshooting, dashboarding, creating basic and advanced rules & analytical models, creation and customisation of reports &queries etc. 20. Complete system level frontend and backend management & maintenance related knowledge need to be transferred to the Bank's staff by the bidder's onsite L1 & L2 resources. 21. There should not be disruption or degradation in the Bank's network bandwidth utilization and availability due to excessive log transmission. 22. Conduct health check-up of the proposed systems by respective OEMs, refer section OEM Services & Deployment. The recommendations in the report should be rectified by	Kindly confirm whether automated, encrypted, versioned backups of all security configurations, detection content, playbooks, dashboards, parsers and integration mappings, with periodic restore tests are needed to be done.	The bidder/OEM shall ensure automated, encrypted and version-controlled backup of all critical security configurations and security content required for restoration and continuity of the proposed solution, including, as applicable, detection rules/use cases, playbooks, dashboards, parsers, correlation rules, queries, workflows, integration mappings and other relevant custom configurations developed for the Bank.
687	78-80	7.13 / AI/ML	AI Explainability	6. Every technology deployed should transform itself from a purely rule based system to analytics & AI/ML based correlation system for logs, vulnerabilities & threat intelligence together for accurate risks prediction. 7. To ensure efficient utilization and monitoring of proposed solution, optimizing capacity utilization, ensuring quality of data and system performance is maintained optimal, there are no security events omission, misfiring rules, heavy rules and reports etc. 8. Participate and contribute in every DR drill, cyber security drill, tabletop exercises by the Bank, regulators or any third party. 9. Conduct DR drill of the Security on quarterly interval or as and when required by the Bank. Ensure DC & DR are exact replica of each other in every manner. 10. Develop custom plug-ins, parsers, connectors, agents, adopters for all the systems in the Bank or related to the Bank periodically or as and when needed. 11. Develop the baseline for the level of logs to be enabled across the different components of IT including infrastructure, databases, business applications and devices etc. The log baselines should be in line with global best practices including NIST, SANS etc. 12. Perform monthly gap analysis of current levels of logs enabled in OS, databases, web servers, business applications and devices and entire	Bidder requests more details on explainability for material AI-driven detections or risk scores, including contributing features, model version, confidence and analyst override capability.	The bidder/OEM shall ensure automated, encrypted and version-controlled backup of all critical security configurations and security content required for restoration and continuity of the proposed solution, including, as applicable, detection rules/use cases, playbooks, dashboards, parsers, correlation rules, queries, workflows, integration mappings and other relevant custom configurations developed for the Bank.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
688	77-79	7.13 / SOC Operations	Threat Hunting	17. Define formats for MIS reporting that includes daily, weekly and monthly or any periodical or adhoc reports, dashboards as per the Bank's requirements. 18. Devise rules, AI/ML based models to analyse logs received from business applications to alert application owners about potential security threat / incident. OWASP and other threat modelling must be used for creating such rules, models. A minimum 15 unique use cases should be developed and implemented for each business application within first six months of go live date. 19. Transfer the knowledge to the Bank's employees about day-to-day operations, system / backend level troubleshooting, dashboarding, creating basic and advanced rules & analytical models, creation and customisation of reports &queries etc. 20. Complete system level frontend and backend management & maintenance related knowledge need to be transferred to the Bank's staff by the bidder's onsite L1 & L2 resources. 21. There should not be disruption or degradation in the Bank's network bandwidth utilization and availability due to excessive log transmission. 22. Conduct health check-up of the proposed systems by respective OEMs, refer section OEM Services & Deployment. The recommendations in the report should be rectified by	Kindly confirm the minimum number of proactive threat-hunting hypotheses per month, mapped to current threat intelligence and MITRE ATT&CK, with findings converted into detections where applicable.	The bidder/OEM shall conduct proactive threat hunting on a periodic basis, using current and relevant threat intelligence and mapping the hunting hypotheses The threat-hunting activities shall be based on the latest available threat intelligence, including relevant OEM/vendor intelligence, CERT-In advisories, MITRE ATT&CK and other credible sources. The bidder/OEM shall document the hypothesis, intelligence/TTP reference, scope, data sources, methodology, findings and recommended actions.
689	75-76	7.12.4 / 7.12.5	Minimum Onsite Manpower	4. The proposed environment shall operate on a 24x7x365 basis. Accordingly, all deployed resources shall be capable of working in rotational shifts, extended hours, weekends, holidays, and during critical situations as required by the Bank. 5. The resource quantities specified in this RFP represent the minimum deployment requirements. The bidder shall appropriately right-size and augment onsite and offsite resources at no additional cost to ensure compliance with SLA, business continuity, operational, and security requirements. 6. All deployed resources shall be named resources. Any replacement, withdrawal, reassignment, or removal of a resource shall require prior written approval from the Bank. 7. In case of resource replacement, the bidder shall ensure an appropriate transition and knowledge transfer period as follows: o Project Manager/L3 (During Operations): Minimum 60 days o Key Personnel (L1/L2): Minimum 45 days o Other Personnel: Minimum 30 days 8. The Bank reserves the right to interview, evaluate, approve, reject, or seek replacement of any proposed or deployed resource. The bidder shall replace any resource found unsuitable, underperforming, non-compliant, or in violation of the Bank's policies within the timeline prescribed by the Bank. The non-availability	We request bank to reconsider the manpower requirements and revise the minimim manpower to run the 24*7 operations for all Solutions and Services.	The Resource requirement given in the RFP is minimum mandatory requirement that is to be deployed. It includes both DC & DR. Bidder can propose the manpower over and above if required.
690	73-75	7.12	OEM Resources	The Bank may require additional onsite resources during the contract period. Such resources shall be provided by the bidder at the pro-rata rates quoted in the Commercial Bill of Material, unless otherwise specified in the RFP. The bidder shall remain solely responsible for ensuring adequate staffing levels and deployment of additional resources required to meet project timelines, operational requirements, service levels, and business continuity requirements throughout the contract period. # Resource Type Deployment Minimum Qualification & Experience Implementation Phase 1 Project Onsite (Full • Graduate/B.E./B.Tech/MCA with PMP/PRINCE2 Manager – Time) or equivalent certification. Implementation • Minimum 8 years of experience • Proven experience in managing at least two Security Solution implementations (including at least one Perimeter Security solution) in PSU/PSE/Government/BFSI/Regulatory organizations. 2 OEM Onsite (Full OEM shall submit a detailed resource deployment Implementation Time) plan before commencement of requirement Resources gathering. Any replacement or modification shall require prior Bank approval.	Please clarify the expected minimum number/duration of OEM onsite resources for each solution during implementation and O&M. Please also confirm whether remote OEM SME support will be acceptable for solutions where the OEM's standard support model is remote.	As mentioned in RFP, implementation is to be done by OEM only for all the solutions and services. Hence, Bidder to right size the resources required for the succeasfull implemention. Please refer section 7.12 Resource Requirement.
691	71	7.11 Warranty, ATS and AMC	Warranty Period vs Staggered Go-Live / AMC Year 4-5	7.11 Warranty, ATS and AMC: The proposed hardware/appliances shall include a comprehensive warranty of three (3) years commencing from the respective Go-Live date. The bidder shall separately quote comprehensive AMC charges for Year 4 and Year 5. The rates quoted by the bidder for hardware, software, licenses, subscriptions, ATS, AMC, and related services shall remain applicable on a pro-rata basis for any additional quantities or services procured during the contract period.	Since different solutions/products are expected to achieve Go-Live on different dates within the 5-month implementation period, please confirm that the 3-year warranty and subsequent Year-4/Year-5 AMC for each hardware component will be computed independently from that component's own Go-Live date, rather than from a single project-level Go-Live date.	The applicable warranty, as sought in the RFP, shall commence from the respective approved Go-Live date of the respective solution. AMC/ATS shall accordingly follow the applicable warranty period.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
692	70-71	7.10 Data Privacy - Executive Governance	Governance Meeting Cadence, Attendance and Cost	7.10 Executive Governance and Project Oversight (item 2): The Project Sponsor, Project Director, and designated senior representatives of the bidder and OEMs shall participate in governance meetings, executive reviews, strategy workshops, and escalation meetings as required by the Bank. On quarterly/or as per the frequency defined by bank, executive governance meetings shall be conducted throughout the contract period.	Please confirm the expected minimum/maximum frequency of executive governance meetings for commercial planning purposes, whether OEM senior representatives are expected to attend in person or may attend virtually, and that any associated travel/logistics costs are included in the quoted price rather than billed separately.	The Bank shall conduct executive governance/review meetings periodically, as required based on the project, operational and governance requirements, and may also convene additional/ad-hoc meetings wherever considered necessary.
693	68-70	7.7 / Cloud	Dedicated Tenant	1. The security telemetry received by the OEM Cloud platform will be routed to the dedicated tenant/workspace provisioned for the Bank. 2. The dedicated tenant/workspace will contain the configurations, policies, security data and analytics applicable to the Bank. 3. All security logs, telemetry, alerts, incidents, configurations, investigation data and other Bank-related security information stored in the Cloud environment shall be encrypted at rest using industry-standard encryption mechanisms. 4. The proposed Cloud/SaaS solution shall support Bring Your Own Key (BYOK) and/or Customer-Managed Encryption Key (CMEK) capability, enabling the Bank to maintain control over the cryptographic keys used to protect its security data.. 5. The encryption key will be securely managed and access to the key will be restricted to authorised personnel/processes. 6. The bidder/OEM shall establish and manage a dedicated cloud landing zone, including Development, UAT, and Production environments, with appropriate segregation, governance, access controls, monitoring, and SDLC controls. 7. The bidder/OEM shall be responsible for provisioning, configuration, administration, monitoring, patching, upgrading, backup, recovery, migration, and lifecycle management of all cloud	Please clarify whether logical tenancy is acceptable or whether the Bank requires dedicated compute/storage/network resources for security-sensitive workloads; please require bidders to disclose all shared infrastructure and isolation controls.	Logical tenancy is acceptable, provided that the proposed bidder/OEM ensure clear separation and isolation of the Bank's data, security telemetry, logs, alerts, configurations, policies, analytics, investigation data and other Bank-related information from those of other tenants. The proposed environment for bank are protected against confidentiality and integrity risks and co-mingling of data and bidder/OEM implement adequate safeguards against combining of information, documents, records and assets.
694	68-70	7.7 / AI Data	AI Data Usage	1. The security telemetry received by the OEM Cloud platform will be routed to the dedicated tenant/workspace provisioned for the Bank. 2. The dedicated tenant/workspace will contain the configurations, policies, security data and analytics applicable to the Bank. 3. All security logs, telemetry, alerts, incidents, configurations, investigation data and other Bank-related security information stored in the Cloud environment shall be encrypted at rest using industry-standard encryption mechanisms. 4. The proposed Cloud/SaaS solution shall support Bring Your Own Key (BYOK) and/or Customer-Managed Encryption Key (CMEK) capability, enabling the Bank to maintain control over the cryptographic keys used to protect its security data.. 5. The encryption key will be securely managed and access to the key will be restricted to authorised personnel/processes. 6. The bidder/OEM shall establish and manage a dedicated cloud landing zone, including Development, UAT, and Production environments, with appropriate segregation, governance, access controls, monitoring, and SDLC controls. 7. The bidder/OEM shall be responsible for provisioning, configuration, administration, monitoring, patching, upgrading, backup, recovery, migration, and lifecycle management of all cloud	Will OEMs need to contractually on their letter head confirm that prompts, telemetry, logs, configurations and incident data will not be used to train shared or external models, including by subprocessors.	The bidder/OEM shall provide the required undertaking on its letterhead, duly authorised by its competent signatory, during the contract period as and when required by the Bank.
695	68	7.7 On-cloud proposed solution OEM Responsibilities	Key Management System Option	7.7 On-cloud OEM Responsibilities (item 13): The solution should provide encryption of data at rest, motion, and in transit using industry-standard cryptographic controls and shall support key management through CSP-native KMS and/or the Bank's Key Management System.	Please clarify whether use of the Bank's own external Key Management System (as opposed to CSP-native KMS) is mandatory for any category of solution, and if so, specify the required integration protocol/standard (e.g., KMIP, PKCS#11) that proposed solutions must support.	The solution shall support the applicable security and key-management architecture specified by the Bank. During the course of the contract, the Bank may provide its own Key Management System (KMS). In such an event, the proposed solution shall support seamless integration with the Bank-provided KMS and comply with the Bank's applicable security, encryption, key-management, and integration requirements.
696	66	7.6.7 / Training	Training	The bidder shall submit a detailed Training and Certification Plan covering training objectives, curriculum, skill levels, training schedules, participant eligibility, certification pathways, and assessment criteria. The training program shall cover product functionalities, administration, troubleshooting, maintenance, security best practices, automation, advanced threat scenarios, security monitoring and analysis, incident response and investigation, threat detection and hunting, intelligence analysis, new features, upgrades, operational workflows, and relevant industry trends. Bidder along with the OEM should provision the training & certification of the bank's relevant officials from the relevant Cloud service provider where the OEM SIEM solution is hosted covering the following Certifications (respectively):	Kindly confirm the minimum requirements for training including total resources to be trained, training duration etc.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
697	65-66	7.6.6.1 / Testing	Performance Testing	7.6.6.1 Quality Assurance 1. Testing Requirements a. The respective OEM shall be responsible for planning, executing, documenting, and successfully completing all testing activities required to validate the functionality, performance, stability, reliability, security, interoperability, and operational readiness of the proposed solution. The bidder shall prepare detailed test plans, test cases, test data, automation scripts (where applicable), entry and exit criteria, test reports, defect logs, root cause analysis reports, workarounds, and remediation plans, and shall obtain the Bank's approval wherever required. 2. Test Preparation The respective OEM shall: a. Prepare the overall testing strategy and methodology for Unit Testing (UT), UAT, Performance Testing, Security Testing, and other applicable tests. b. Establish and maintain the required test environments, infrastructure, software, applications, and test data. c. Prepare, validate, and execute test cases, scripts, and automation frameworks, wherever applicable. d. Define test entry and exit criteria, acceptance criteria, and success parameters. 3. Test Execution The respective OEM shall: a. Execute all approved test cases and scripts. b. Record, track, report, and resolve defects, deviations, and observations. c. Perform re-testing and regression	Will bank provide any performance testing tools for load trsting etc. Kindly confirm.	The bidder/OEM shall provide all tools, utilities, scripts, infrastructure and resources necessary to perform the testing required under the RFP unless the Bank specifically confirms otherwise.
698	57	7.4.9 Brand Protection and Monitoring	Brand Protection Takedown SLA & Coverage	7.4.9 Brand Protection and Monitoring: The Bidder shall provide offsite, tool-based continuous brand protection and digital risk monitoring services... including continuous monitoring for brand impersonation, domain monitoring for typosquatting and look-alike domains, monitoring of fraudulent mobile applications, social media monitoring, and takedown coordination with relevant registrars, hosting providers, platforms, application stores, social media platforms, and other relevant entities, wherever applicable.	Please define the target takedown SLA by asset type (domain, mobile app listing, social media profile) and confirm the minimum number of digital channels/platforms (app stores, social media platforms, domain registrars) that must be monitored under this service at no additional cost.	Please refer addendum for revised clause
699	56	7.4.5 Anti-Phishing	Anti-Phishing Detection-to-Takedown SLA	7.4.5 Anti-Phishing: The Bidder shall provide offsite continuous anti-phishing monitoring and response services for detection, analysis for phishing attacks targeting the Bank, its employees, customers, executives, digital assets, domains, and online channels, including continuous detection and monitoring of phishing websites, domains, emails, URLs, and fraudulent content, and monitoring and identification of brand and domain impersonation.	Please specify the required detection-to-notification and notification-to-takedown SLA for confirmed phishing/impersonating domains and sites, and confirm whether registrar/hosting-provider takedown coordination and associated costs are included in the quoted price.	Please refer to the relevant Addendum for updated specfications
700	55-60	7.6 / Deception	Deception	7.6.1 Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder) 1. The respective Solution OEM, assisted by the bidder, shall conduct a detailed assessment of the Bank's business, functional, technical, operational, security, compliance, and integration requirements and design a scalable, resilient, and future- ready solution. The proposed solution shall fully comply with the requirements specified in the RFP and support future business and technology needs of the Bank. 2. As part of the requirement gathering phase, the OEM shall conduct workshops, discovery sessions, interviews, and discussions with the Bank's stakeholders and appointed consultants to understand business requirements, existing infrastructure & solutions, integrations, operational processes, and security requirements. 3. The OEM shall review the Bank's existing IT, security, application, network, cloud, and infrastructure landscape and recommend an optimized target-state architecture leveraging both existing and proposed components wherever feasible. 4. The OEM shall identify all required data sources, integrations, dependencies, interfaces, telemetry sources, and compliance requirements and prepare a detailed solution architecture and deployment design in	Kindly confirm wherther deception technology should support dynamic decoys, credential lures, lateral-movement detection and high-confidence alerting, with evidence of production deployment at scale.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
701	55-60	7.6 / Cloud Security	CSPM/CNAPP/CWPP	7.6.1 Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder) 1. The respective Solution OEM, assisted by the bidder, shall conduct a detailed assessment of the Bank's business, functional, technical, operational, security, compliance, and integration requirements and design a scalable, resilient, and future- ready solution. The proposed solution shall fully comply with the requirements specified in the RFP and support future business and technology needs of the Bank. 2. As part of the requirement gathering phase, the OEM shall conduct workshops, discovery sessions, interviews, and discussions with the Bank's stakeholders and appointed consultants to understand business requirements, existing infrastructure & solutions, integrations, operational processes, and security requirements. 3. The OEM shall review the Bank's existing IT, security, application, network, cloud, and infrastructure landscape and recommend an optimized target-state architecture leveraging both existing and proposed components wherever feasible. 4. The OEM shall identify all required data sources, integrations, dependencies, interfaces, telemetry sources, and compliance requirements and prepare a detailed solution architecture and deployment design in	Is there a need for unified cloud asset inventory and risk correlation across CSPM, CNAPP and CWPP to prevent duplicate findings and inconsistent ownership. Kindly confirm.	No Change, Please be guided by the RFP
702	55-56	7.4.4 Phishing Simulation	Phishing Campaign Cadence & Scope	7.4.4 Phishing Simulation: The Bidder shall provide offsite, tool-based phishing simulation services to assess employee awareness, measure the Bank's resilience against phishing attacks, and support continuous improvement of security awareness. The service shall include conducting controlled and customizable simulated phishing campaigns, user awareness and susceptibility assessment, department-wise and user-wise risk assessment, campaign-wise and periodic awareness effectiveness reporting, and recommendations for improving employee security awareness including training.	Please specify the minimum number of phishing campaigns per year, the employee/user base to be covered per campaign, and whether campaign design, template creation and remedial training content are to be provided by the bidder at no additional cost.	Please refer 7.2.2 Services for Frequency. The Bidder shall design, in conformity with the bank, the campaign coverage and campaign methodology required to meet the RFP. The proposed service shall support campaigns for the Bank's user base as required by the Bank during the contract period. Campaign design, template creation, reporting and associated activities required to fulfil the RFP shall be included in the Bidder's scope.
703	50-60	7.5 / NDR	NDR 10 Gbps	7.6.1 Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder) 1. The respective Solution OEM, assisted by the bidder, shall conduct a detailed assessment of the Bank's business, functional, technical, operational, security, compliance, and integration requirements and design a scalable, resilient, and future- ready solution. The proposed solution shall fully comply with the requirements specified in the RFP and support future business and technology needs of the Bank. 2. As part of the requirement gathering phase, the OEM shall conduct workshops, discovery sessions, interviews, and discussions with the Bank's stakeholders and appointed consultants to understand business requirements, existing infrastructure & solutions, integrations, operational processes, and security requirements. 3. The OEM shall review the Bank's existing IT, security, application, network, cloud, and infrastructure landscape and recommend an optimized target-state architecture leveraging both existing and proposed components wherever feasible. 4. The OEM shall identify all required data sources, integrations, dependencies, interfaces, telemetry sources, and compliance requirements and prepare a detailed solution architecture and deployment design in	Kindly confirm that 10 Gbps sustained and burst performance demonstration with representative encrypted, east-west and north-south traffic and no material packet loss beyond documented tolerances.	Please refer addendum for revised clause
704	48-55	7.4 / UEBA	UEBA Baseline	16. Restoration of configuration data, audit logs, reports, and operational data from backup for audit, forensic investigation, and regulatory requirements without additional cost to the Bank.	Bidder requests UEBA baselines for adaptive baselining by user, peer group, asset and service account, and to document cold-start, seasonal and sparse-data handling.	Details shall be shared with the successful bidder.
705	41	7.3.1.2 SIEM Data Ingestion and EPS Measurement	EPS Measurement	20. Key administrative and security-sensitive activities, including user access changes and configuration updates, shall be auditable. 21. All ingested customer logs and data shall remain the property of the Bank throughout the contract period and upon expiry/termination. 7.3.1.2 SIEM Data Ingestion and EPS Measurement The proposed solution shall support SIEM sizing based on actual data ingested by the SIEM, measured in Events Per Second (EPS) and/or Daily Data Ingestion (GB/day or TB/day), as applicable. SIEM EPS shall mean the number of unique log records/events actually delivered to and ingested by the SIEM for SIEM processing. EPS shall be measured at the SIEM ingestion boundary, after applicable source-side filtering or selection and at or immediately before the SIEM processing boundary.	Please confirm that capacity/licensing evaluation will be based on the EPS measured at the defined SIEM ingestion boundary and that any source-side deduplication/filtering performed before the SIEM boundary will not create an additional licensing obligation, provided the input/output metrics remain auditable.	Refer Section 7.3.1.2 SIEM Data ingestion and EPS measurement The bidder shall be provided with an on-premise/onsite measurement, collection or monitoring component capable of measuring and reporting the volume of logs/events forwarded towards the SIEM
706	41	7.3.1 SIEM	AI/ML Capabilities	For solutions where XDR (or any other solution) and SIEM capabilities are delivered through a unified security platform, the Bidder shall demonstrate how the proposed architecture avoids duplicate ingestion, duplicate storage, and artificial inflation of SIEM EPS while maintaining the required security analytics and detection capabilities.	Please clarify which AI capabilities are mandatory for technical compliance versus desirable/roadmap capabilities, and whether OEM-native AI features or integrated third-party AI services are acceptable. Please also clarify whether any separate AI/compute infrastructure must be quoted.	No Change, Please be guided by the RFP. Bidder is required to righst size and design the solution factoring all the required compenent to meet the Functionality as defined in RFP and Appendix

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
707	37-43	7.2.3 / SIEM	Retention	Requirement Requirement Details required resources to support the specified log ingestion, processing, retention and recovery requirements throughout the contract period. Primary Log • Raw SIEM logs shall be retained on the Cloud-designated primary Storage & storage for a minimum period of 1 month in their Retention original/unmodified form, along with relevant timestamps, source information and metadata. • Parsed, normalized, enriched, indexed and correlated logs, together with associated metadata and contextual information, shall be retained for a minimum period of 60 months (5 years). • The Bidder shall provision adequate storage considering ingestion volumes, growth, processing, indexing, retention and applicable overheads. Backup, • The Bidder/OEM shall manage the required backup at the Recovery & DR CSP/Cloud site for SIEM availability and recovery. • In addition, raw and processed/normalized SIEM logs, configurations, policies, rules, metadata and other Bank-owned SIEM data shall be backed up/transferred to the Bank's designated backup infrastructure at DC and DR in accordance with the Bank's Backup and Data Retention Policy (refer Annexure 21).	Please clarify the exact retention tier for searchable hot data, warm data, archive and backup, and require bidders to state the searchable retention period and retrieval SLA for each tier.	Please refer addendum for the revised clause
708	37-43	7.2.3 / SIEM	Retention Integrity	Requirement On-Premises Deployment of solutions On-Premises • The solution shall be deployed within the Bank's designated Deployment Primary Data Centre (DC/NDC) and Secondary Disaster Recovery Centre (DR/NDR). • The Bidder/OEM shall provide all required application components, management components, databases, storage, collectors, brokers, agents, consoles and other components necessary for the complete solution. Raw Log / Data • The solution shall store applicable logs, data, databases, Storage on metadata and other solution-generated information on the Bank- Primary Storage designated primary storage for the retention period specified in this RFP. Where logs are generated or collected, raw logs shall be retained in their original/unmodified form, along with relevant timestamps, source information and associated metadata. Backup Storage / • Backup of application binaries, operating systems, databases, Appliance configurations, policies, rules, workflows, dashboards, metadata and other solution components shall be performed using the proposed designated backup infrastructure and backup solution. The Bidder/OEM shall provide all required backup agents, connectors, utilities and configuration necessary for the proposed solution. Backup of Logs / • Required logs, security data,	Please require cryptographic integrity protection, tamper evidence and chain-of-custody controls for retained logs, including validation that archived logs have not been altered.	No Change, Please be guided by the RFP
709	37	7.2.3 / SIEM	SIEM Data Retention	Requirement Requirement Details required resources to support the specified log ingestion, processing, retention and recovery requirements throughout the contract period. Primary Log • Raw SIEM logs shall be retained on the Cloud-designated primary Storage & storage for a minimum period of 1 month in their Retention original/unmodified form, along with relevant timestamps, source information and metadata. • Parsed, normalized, enriched, indexed and correlated logs, together with associated metadata and contextual information, shall be retained for a minimum period of 60 months (5 years). • The Bidder shall provision adequate storage considering ingestion volumes, growth, processing, indexing, retention and applicable overheads. Backup, • The Bidder/OEM shall manage the required backup at the Recovery & DR CSP/Cloud site for SIEM availability and recovery. • In addition, raw and processed/normalized SIEM logs, configurations, policies, rules, metadata and other Bank-owned SIEM data shall be backed up/transferred to the Bank's designated backup infrastructure at DC and DR in accordance with the Bank's Backup and Data Retention Policy (refer Annexure 21).	Please clarify whether the 60-month retention requirement applies to all SIEM data in searchable/hot storage or whether archived/cold storage is acceptable, with restoration/search capability within an agreed RTO. This clarification is important for consistent sizing and TCO comparison.	Please refer addendum for revised clause
710	35-36	7.2.4.2 Connectivity and Data Flow	Bandwidth, Latency and Redundancy for Cloud Connectivity	7.2.4.2 Connectivity and Data Flow: The collected telemetry and security data shall be securely transmitted to the applicable Cloud/SaaS security platforms through controlled connectivity mechanisms, including Firewall/NGFW, Secure Internet Gateway, Private/Direct Connectivity, VPN/IPSec and TLS 1.2+ encrypted communication, as applicable.	Please specify (or confirm bidder is to propose and justify) the minimum bandwidth, latency and redundancy requirements for connectivity between the Bank's DC/DR/branches and the Cloud/SaaS platforms sufficient to sustain the peak EPS/data-ingestion volumetrics specified in Annexure 21, and confirm whether dedicated/private connectivity (e.g., ExpressRoute/Direct Connect/MPLS) charges are to be included in the bidder's quoted price.	The bidder shall independently determine and provision connectivity adequate to meet the stated volumetrics, performance and SLA requirements.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
711	32-37	7.2 / 7.3	Cloud Data Egress / Exit	7.2.4.3 Storage and other Requirement On Cloud Solutions 1. General requirement for all cloud deployed solutions a. Long-Term Storage - Long-term archival of applicable logs, security data, metadata, reports, audit information and other relevant information shall be maintained on the Bank's designated long-term archival infrastructure. The solution shall support secure transfer, retrieval and restoration of archived information throughout the applicable retention period. b. Storage Capacity & Sizing - The Bidder shall provide detailed storage sizing based on expected data/log volumes, peak ingestion rate, retention period, indexing, enrichment, compression, replication, backup, archival and anticipated annual growth. Adequate capacity shall be provided for the complete contract period. c. No Bank data shall be deleted or made inaccessible before expiry of the applicable retention period (refer annexure 21) and without explicit written authorization from the Bank. d. InGress and Egress - All data ingress and egress associated with the solution shall be provided at no additional cost to the Bank, including log/data ingestion, API traffic, integrations, backup, replication, archival, restoration, data retrieval, export, migration and exit/transition. The Bidder shall include all applicable Cloud provider	Please clarify the expected exit/transition data volume and required export format for SIEM and other solutions. Please also confirm whether the Bank expects the bidder to bear third-party CSP egress charges without limit or whether a defined transition/exit volume will be specified.	The bidder shall support complete and usable extraction/ transition of Bank-owned data required for continuity, regulatory, audit and exit purposes. Data shall be provided in industry-standard, documented, machine-readable/native formats, as applicable to the solution. The bidder shall not impose artificial technical restrictions on extraction. The Bank may specify a transition plan and data set during exit. All required ingress/egress cost is part of the bidder's scope
712	29-31	7.2.1 Master Deployment Matrix	HA / Failover	Note: For solutions deployed in Cloud (SaaS) + Hybrid mode, any agents, sensors, collectors, connectors, brokers, aggregators, gateways, enforcement components or other components required to be deployed within the Bank's infrastructure for collection, processing, integration, monitoring or enforcement shall be provided, deployed, configured, maintained and supported by the Bidder/OEM as part of the proposed solution and shall be included in the quoted cost. Where N+N Active-Active HA is mandated, all applicable critical Bank-deployed components shall comply with the prescribed HA architecture at DC and DR. The underlying Cloud (SaaS) platform shall provide appropriate cloud-native HA, geographic resiliency and DR in accordance with the	Please define the maximum acceptable failover time in seconds and the acceptance-test methodology for demonstrating HA/failover for each solution. Please also clarify whether both DC and DR are required to operate Active-Active for all applicable components.	No Change, Please be guided by the RFP
713	26-28	7.1 / Scope	Integration with Future Tools	integration, playbook development, reporting customization, alert tuning, remediation activities, APIs, or native integrations required for successful implementation shall be provided without any additional cost to the Bank throughout the contract period. a. Key Implementation Responsibilities a. The implementation of each proposed solution, including design, installation, configuration, integration, migration, testing, commissioning, user acceptance testing (UAT), and Go-Live, shall be performed by the respective OEM. The Bidder shall arrange OEM resources, coordinate implementation activities, and ensure timely completion of the project. b. Upon successful implementation, the respective OEM shall provide a certificate confirming that the solution has been deployed by the OEM and complies with all functional and technical requirements specified in the RFP and SRS. b. Key Roles and Responsibilities: a. System Integrator (Bidder): o Supply all proposed solutions. o Manage the overall project. o Coordinate with all OEMs and third parties. o Provide onsite L1, L2, and L3 support resources. o Perform implementation coordination, documentation, knowledge transfer, training, and project governance. b. Solution OEM: o Design, deploy, integrate, test, commission, configurations/data/logs, optimize	Please clarify the boundary of this obligation and confirm that integrations with future tools not identified in the RFP, or requiring new OEM licenses/connectors/custom development, will be handled through mutually agreed change control and applicable commercial rates.	The requirement for integration and associated activities shall apply to all integrations, interfaces, APIs, connectors, playbooks, alert tuning, reporting customization and remediation activities required for successful implementation, operation and interoperability of the solutions within the scope of this RFP, including integration with the Bank's existing infrastructure, security tools, platforms and technologies identified in the SRS. The Bidder/OEM shall provide the required integration, configuration, API utilization, connector/interface development and related activities without any additional cost to the Bank where such activities are necessary to meet the functional and technical requirements specified in the RFP/SRS and to achieve the intended integrated SOC functionality at no additional cost to the bank.
714	26-28	7.1 / Scope	Customization / API / Playbooks	integration, playbook development, reporting customization, alert tuning, remediation activities, APIs, or native integrations required for successful implementation shall be provided without any additional cost to the Bank throughout the contract period. a. Key Implementation Responsibilities a. The implementation of each proposed solution, including design, installation, configuration, integration, migration, testing, commissioning, user acceptance testing (UAT), and Go-Live, shall be performed by the respective OEM. The Bidder shall arrange OEM resources, coordinate implementation activities, and ensure timely completion of the project. b. Upon successful implementation, the respective OEM shall provide a certificate confirming that the solution has been deployed by the OEM and complies with all functional and technical requirements specified in the RFP and SRS. b. Key Roles and Responsibilities: a. System Integrator (Bidder): o Supply all proposed solutions. o Manage the overall project. o Coordinate with all OEMs and third parties. o Provide onsite L1, L2, and L3 support resources. o Perform implementation coordination, documentation, knowledge transfer, training, and project governance. b. Solution OEM: o Design, deploy, integrate, test, commission, configurations/data/logs, optimize	Please clarify whether the no-additional-cost obligation is limited to requirements explicitly described in the RFP and integrations listed in the Bank's current environment, and whether future/new integrations or material custom development will be treated through change control.	The requirement for integration and associated activities shall apply to all integrations, interfaces, APIs, connectors, playbooks, alert tuning, reporting customization and remediation activities required for successful implementation, operation and interoperability of the solutions within the scope of this RFP, including integration with the Bank's existing infrastructure, security tools, platforms and technologies identified in the SRS. The Bidder/OEM shall provide the required integration, configuration, API utilization, connector/interface development and related activities without any additional cost to the Bank where such activities are necessary to meet the functional and technical requirements specified in the RFP/SRS and to achieve the intended integrated SOC functionality at no additional cost to the bank.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
715	258-262	16.21.2 / 16.21.3	Backup and LTS	Backup Type Retention Location Retention Period Duration of the Long-Term Storage (LTS) Entire Duration Contract (Monthly Full of the Contract backup) Note: Upon completion of the two (2) month retention period on the Backup Storage, the applicable Monthly Full Backups shall be migrated to Long-Term Storage (LTS) at bank's DC & DR and retained for the entire duration of the contract. The Bidder shall provide and deploy the proposed Backup Solution, Backup Storage / Backup Appliance and Long-Term Storage (LTS) at both the Bank's designated Primary Data Centre (DC) and Disaster Recovery Centre (DR).	Please provide the expected daily backup volume/change rate for the proposed SOC environment, or confirm that bidders may use reasonable sizing assumptions based on the RFP volumetrics. Please also clarify whether backup software/storage may be common across multiple solutions.	Bidder and OEM to Design the solution meeting the requirement stated in the RFP
716	258-260	16.21.2 Volumetrics - Solution-wise Requirements	Growth/Scale-up Mechanism for Non-SIEM Solutions	16.21.2 Volumetrics - Solution-wise Requirements specifies fixed baseline capacities for each solution (e.g., XDR: 12,000 users scalable to 14,000; UEBA: 12,000 endpoint users scalable to 16,000; Decoy: minimum 200 applications/networks/devices with 50 segments; CNAPP/CWPP: 20 VPCs/VNets, VM count 100; VA-VM: minimum 4,000 IPs; ITDR/CTEM: 12,000 users scalable to 16,000, 4,000 IPs). Only SIEM specifies a defined tranche-based commercial mechanism (10,000 EPS/420 GB per day tranches) for capacity beyond the base and scalable figures.	Please confirm the defined tranche/unit and BOM-quoted rate for procuring additional capacity beyond the stated scalable ceiling for each non-SIEM solution (XDR, UEBA, Decoy, CNAPP, CWPP, VA-VM, ITDR, CTEM, CSPM), consistent with the tranche mechanism specified for SIEM, so that bidders quote on a like-for-like commercial basis for future growth.	Please refer addendum for revised clause
717	258-259	16.21.2 Volumetrics	DC and DR Capacity	Each node/environment must be individually provisioned for full peak load	Please clarify whether DC and DR must each independently support the full 50,000 EPS base and 75,000 EPS scalable capacity, or whether the DR environment can be sized differently based on the prescribed DR operating mode/RTO/RPO.	Please refer addendum for revised clause
718	258	16.21.2 Volumetrics	SIEM Volumetrics	Total 50,000 sustainable EPS/ 2.06 TB per day (whichever is higher) of data ingestion from the outset scalable to Total 75,000 sustainable EPS/ 3.09 TB per day (whichever is higher) at DC & DR. Each node/environment must be individually provisioned for full peak load The bank will procure additional Licenses in the tranches of 10,000 EPS/ 420 Gb per day based on the rate provided in the BOM.	Please confirm whether the mandatory base SIEM license/capacity to be quoted is 50,000 EPS (or 2.06 TB/day, whichever is higher), and whether the 75,000 EPS capacity is to be physically provisioned from Day-1 or only made scalable through additional 10,000-EPS tranches.	Please refer addendum for revised clause
719	258	16.21.2 Volumetrics	SIEM EPS and Data Volume Conversion	Note: Average Event Size considered is 500 Bytes per Event	Please confirm the intended unit convention (decimal TB vs TiB) and the authoritative sizing basis for commercial evaluation. At 50,000 EPS and 500 bytes/event, the calculated daily volume is approximately 2.16 TB/day using decimal units.	No Change, Please be guided by the RFP
720	258	16.21.2 Volumetrics	Additional SIEM Licenses	The bank will procure additional Licenses in the tranches of 10,000 EPS/ 420 Gb per day based on the rate provided in the BOM.	Please confirm that additional capacity beyond the initial quoted requirement will be ordered only when required by the Bank and billed at the unit rates quoted in the BoM, and that no unused capacity commitment is expected.	The SIEM is being procured as a SaaS solution. Additional capacity shall be procured in 10,000 EPS / 420 GB/day tranches. The quoted rates shall include the required cloud infrastructure, storage, compute, connectivity and associated data-transfer costs as specified in the RFP.
721	258	16.21.2 Volumetrics (SOAR)	SOAR Concurrent User Licensing	16.21.2 Volumetrics - SOAR: 5 Concurrent users/Analyst. There should be no limitation/restriction on SOAR licenses based on the number of events coming to the SOAR or the number of playbooks or actions performed by SOAR.	Please confirm whether 5 concurrent SOAR users is the firm baseline for a 24x7x365 multi-shift SOC team, or whether the bidder should size concurrent licenses based on actual shift strength; please also confirm the incremental cost basis if additional concurrent seats are required.	Bidder to right size as per the RFP
722	256-257	16.21.1 Current IT Assets / 7.1 Scope	Legacy SOC/SIEM Decommissioning & Historical Log Migration	16.21.1 Current IT assets lists the Bank's centralized IT infrastructure, databases, applications, branch desktops and network devices to be onboarded (tentative counts: 2,500 servers, 300 databases, 200 applications, 12,000 desktops, 7,200 routers/switches). Section 7.1 requires log ingestion, processing, retention (60 months) and recovery for the proposed NextGen SOC solutions throughout the contract period.	Please confirm whether an existing SIEM/SOC platform is currently operational and being replaced under this RFP, and if so: (a) whether historical logs/data from the legacy platform must be migrated into the new solution and for what retention period, (b) the expected parallel-run/cutover duration, and (c) whether parallel-run licensing/infrastructure costs for the outgoing and incoming platforms are to be borne by the bidder.	Yes, the existing SIEM/SOC platform is operational and will be replaced under this RFP. No historical data migration from the existing SIEM is envisaged. The existing SIEM/SOC infrastructure and solution shall be operated and maintained by the bidder on an "as-is, where-is" basis during the parallel-run period, as required for compliance, at no additional cost to the Bank. The existing SIEM shall continue to be operated for a period of 12 months after Go-Live of the proposed SIEM, primarily to support regulatory, audit and transition requirements.
723	253-255	16.20 Annexure 20	S-BOM / C-BOM	16.20 Annexure 20: S-BOM & C-BOM DETAILS of all the proposed Tool/solutions a. S-BOM On OEM Letterhead S.No. Component Component Component Component Component Component Component Name Name Name Name Name 1. Version 2. Description 3. Supplier 4. License 5. Origin 6. Dependencies 7. Vulnerabilities 8. Patch Status 9. Release Date 10. End of Life Date	Please clarify the minimum level of SBOM/CBOM detail expected at bid stage, particularly where OEMs cannot disclose proprietary/deep dependency information before award due to confidentiality restrictions. Please confirm whether a public/standard SBOM can be submitted at bid stage with detailed/private SBOM to be provided post-award.	Please refer Annexure 18: Compliance with FRS, TRS, SoW & SBOM (on respective OEM letterhead), Point 5
724	221-223	16.8 Annexure 8	OEM Commitments	16.8 Annexure 8: Certification on OEM Requirements RFP No.: _____ f(Letter to be submitted on the OEM's letterhead) To, General Manager (Cyber Security) Staff Training Centre Punjab & Sind Bank CISO Cell, 3rd Floor B-8/232, Naharpur Village Road, Pocket 8, Sector 3B Rohini, Delhi – 110085	Please clarify whether the OEM is expected to deploy full-time onsite resources throughout implementation and O&M or only provide resources/SMEs on demand as per the agreed resource deployment plan. Please also clarify which OEM commitments are contractual obligations of the bidder versus direct OEM obligations.	As mentioned in RFP, implementation is to be done by OEM only for all the solutions and services. Hence, Bidder to right size the resources required for the succeasfull implemention. Please refer section 7.12 Resource Requirement.
725	220-221	16.7 / 16.8 Annexures	MAF / Annexure Numbering	16.7 Annexure 7: Minimum Local Content Certification Format for Affidavit of Self certification regarding Local Content in line with PPP-MII order and MoP Order, if applicable, to be provided on a non-judicial stamp paper of Rs. 100/-.	Please clarify and issue a corrected Annexure 7/MAF format. In particular, please confirm whether a separate OEM Manufacturer Authorization Form is mandatory in addition to Annexure 8 and Annexure 18. There is no format for MAF given in the RFP as such. Kindly share the MAF format.	Separate OEM Manufacture Authorization form is mandatory in addition to Annexures.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
726	216-217	General Eligibility Conditions	Production Deployment Experience	t. The bidder and/or OEM shall comply with applicable guidelines issued by the Central Vigilance Commission (CVC), including Circular No. 03/01/12, the applicable provisions of the General Financial Rules (GFR), and the Department of Expenditure Office Memorandum dated 25.07.2016, as amended from time to time. u. In a tender, either the Indian Agent on behalf of the Principal/OEM or the Principal/OEM itself may bid; however, both shall not bid simultaneously for the same item/product in the same tender. v. Documentary evidence shall be furnished against each eligibility criterion along with a detailed index of documents submitted. All documents shall be duly signed and stamped by the Authorized Signatory of the bidder. Relevant sections of the submitted documents supporting compliance with the eligibility criteria shall be clearly highlighted for ease of verification by the Bank. w. Any misrepresentation, suppression of facts, submission of forged/fabricated documents, or provision of incorrect information by the bidder at any stage of the bidding process may result in rejection of the bid, forfeiture of bid security (if applicable), and/or blacklisting/debarment from participating in future procurement processes of the Bank, without prejudice to any other rights and remedies available	Please clarify whether a multi-solution SOC deployment can be used to demonstrate experience for multiple categories where each solution is independently deployed and the client-issued evidence clearly identifies the respective solution, scope and production use.	Experience of solutions can be shown in single /multiple Clients/ work orders meeting the above criteria
727	17-18	6.4.1	Masked BoM	6.4 Two Bid System: This is two bid system which has the following 2 parts: Part A- Technical cum Eligibility Proposal: Indicating the response to the Pre-Qualification Criteria, Technical evaluation criteria, Appendix & annexures for Technical and Eligibility requirement, Compliance to Scope of Work and other terms & conditions. The format for submission of Technical Proposal is as per Annexure 1: Submission checklist along with Appendix 1: Functional Compliance Sheet and Appendix 2: Masked Bill of Material. Part B-Commercial Bid: Furnishing all relevant information as required as per Bill of Material as per Appendix 2. 6.4.1 Preparation for Bids: 6.4.1.1 Part A – Technical cum Eligibility Proposal 1. Before submitting the bid, the bidders should ensure that they have reviewed the terms and conform to the Pre-Qualification Criteria as stated in RFP. Only after satisfying themselves with the Pre-Qualification Criteria, the Offer should be submitted. 2. Technical cum eligibility Proposal should be submitted as per the format in Annexure 1: Submission Checklist. Relevant technical details and documentation should be provided along with Technical Proposal. 3. It is mandatory to provide compliance with the scope, requirements, and terms required by the bank. 4. The offer may not be	Please confirm whether OEM part numbers/SKUs, license metrics, subscription terms and support/ATS/AMC line items must remain visible in the Masked BoM.	Yes, Your understanding is correct.
728	168	14.24 / Audit	Audit Remediation	14.24 Audit by Third Party The selected bidder (Service Provider), if required, has to get itself annually audited by internal/external empaneled Auditors appointed by the Bank/inspecting official from the Reserve Bank of India or any regulatory authority, covering the risk parameters finalized by the Bank/such auditors in the areas of products (IT hardware/software) and services etc., provided to the Bank and the Service Provider is required to submit such certification by such Auditors to the Bank. The Service Provider and/or his/their outsourced agents/subcontractors (if allowed by the Bank) shall facilitate the same. The Bank can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by the Service Provider. The Service Provider shall, whenever required by the Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by the Bank. Where any deficiency has been observed during audit of the Service Provider on the risk parameters finalized by the Bank or in the certification submitted by the Auditors, the Service Provider shall correct/resolve the same at the earliest and shall provide all necessary documents related to resolution thereof and the auditor shall further certify	Please define severity-based remediation timelines for audit findings and process for formal risk acceptance by the Bank for any deferred high-risk finding.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
729	167-168	14.22-14.23 / Termination	Termination for Convenience	3) The Bank reserves its right to invoke the Bank Guarantee/ foreclose the Security Deposit /recover from outstanding amount to the credit of the selected bidder towards the non- performance/non-compliance of the terms and conditions of the contract and/ or to recover the dues payable by the Bidder from any, to appropriate towards damages (as mentioned in Point-1 and Point-2). Bidder's Obligation on termination If the Contract is terminated on Non-Performance/contract expiry then – 1) The Bidder shall handover all documents/ executable/ Bank's data or any other relevant information to the Bank in timely manner and in proper format as per scope of this RFP and shall also support the orderly transition to another vendor or to the Bank. 2) During the transition, the Bidder shall also support the Bank on technical queries/support on process implementation or in case of software provision for future upgrades 3) During the transition, the bidder shall continue to provide services as per the terms of the Agreement until a 'New Service Provider' completely takes over the work. During the transition phase, the bidder shall render all reasonable assistance to the new Service Provider within such period prescribed by the Bank, at no extra cost to the Bank, for ensuring smooth	Please clarify payment for accepted committed licenses, non-cancellable OEM/CSP commitments and approved transition costs incurred before termination, subject to documented mitigation.	No Change, Please be guided by the RFP
730	167-168	14.23 / Exit	Transition	3) The Bank reserves its right to invoke the Bank Guarantee/ foreclose the Security Deposit /recover from outstanding amount to the credit of the selected bidder towards the non- performance/non-compliance of the terms and conditions of the contract and/ or to recover the dues payable by the Bidder from any, to appropriate towards damages (as mentioned in Point-1 and Point-2). Bidder's Obligation on termination If the Contract is terminated on Non-Performance/contract expiry then – 1) The Bidder shall handover all documents/ executable/ Bank's data or any other relevant information to the Bank in timely manner and in proper format as per scope of this RFP and shall also support the orderly transition to another vendor or to the Bank. 2) During the transition, the Bidder shall also support the Bank on technical queries/support on process implementation or in case of software provision for future upgrades 3) During the transition, the bidder shall continue to provide services as per the terms of the Agreement until a 'New Service Provider' completely takes over the work. During the transition phase, the bidder shall render all reasonable assistance to the new Service Provider within such period prescribed by the Bank, at no extra cost to the Bank, for ensuring smooth	Please define a maximum transition period and transition deliverables, and specify that post-term assistance beyond the included period will be payable where not caused by bidder default.	No Change, Please be guided by the RFP
731	165	14.19 / LD	LD Cap	14.19 Liquidated Damages The Bank will consider the inability of the bidder to deliver or install the equipment & provide the services required within the specified time limit as a breach of contract and would entail the payment of Liquidated Damages on the part of the bidder. The liquidated damages represent an estimate of the loss or damage that the Bank may have suffered due to delay in performance of the obligations (relating to delivery, installation, operationalization, implementation, training, acceptance, warranty, maintenance etc. of the proposed solution/services) by the bidder. Installation will be treated as incomplete in one / all the following situations: 1. Non-delivery of any component or other services mentioned in the order 2. Non-delivery of supporting documentation 3. Delivery / availability, but no installation of the components and software 4. No integration/ Incomplete Integration 5. Non-Completion of Transition within suggested timeline 6. System operational, but not as per SLA, Timelines and scope of the RFP If the bidder fails to deliver any or all of the products, systems and services solutions within the time period(s) specified in the Delivery Schedule or installation, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the	Please clarify whether the 10% cap is per category, per milestone or aggregate across all LD/SLA credits, and ensure that recurring service failures are not effectively shielded by a single aggregate cap.	No Change, Please be guided by the RFP RFP Clause 13.2 - For the purpose of this RFP, the total penalties as per LD & SLA will be subject to a maximum of 10% of the overall contract value

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
732	163-168	14 / Contract	Regulatory Change	14.24 Audit by Third Party The selected bidder (Service Provider), if required, has to get itself annually audited by internal/external empaneled Auditors appointed by the Bank/inspecting official from the Reserve Bank of India or any regulatory authority, covering the risk parameters finalized by the Bank/such auditors in the areas of products (IT hardware/software) and services etc., provided to the Bank and the Service Provider is required to submit such certification by such Auditors to the Bank. The Service Provider and/or his/their outsourced agents/subcontractors (if allowed by the Bank) shall facilitate the same. The Bank can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by the Service Provider. The Service Provider shall, whenever required by the Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by the Bank. Where any deficiency has been observed during audit of the Service Provider on the risk parameters finalized by the Bank or in the certification submitted by the Auditors, the Service Provider shall correct/resolve the same at the earliest and shall provide all necessary documents related to resolution thereof and the auditor shall further certify	Please define how newly issued regulatory requirements that materially change scope or technology will be handled through change control without compromising regulatory compliance.	No Change, Please be guided by the RFP
733	163-166	14.13-14.21 / Liability	Cyber Incident Liability	14.21 Limitation of Liability The aggregate liability of bidder in connection with this Agreement, in respect of any claims, losses, costs or damages arising out of or in connection with this RFP/Agreement shall not exceed the total Project Cost. Under no circumstances shall either Party be liable for any indirect, consequential or incidental losses, damages or claims including loss of profit, loss of business or revenue.	Please consider liability cappted to total contract value for data breach, confidentiality breach, IP infringement, fraud, wilful misconduct and regulatory penalties attributable to bidder/OEM, subject to applicable law and Bank policy.	No Change, Please be guided by the RFP
734	163	14.13 / Indemnity	Indemnity	14.13 Indemnity The bidder agrees to indemnify and keep indemnified the Bank against all losses, damages, costs, charges and expenses incurred or suffered by the Bank due to or on account of any claim for infringement of intellectual property rights.	Indemnity obligations should be cappted to overall services / mnapower fee of the Bidder. Request Bank's reconsideration.	No Change, Please be guided by the RFP
735	161	14.8 / DPDP	Data Protection	14.7 Legal Compliance The successful bidder hereto agrees that it shall comply with all applicable union, state and local laws, ordinances, regulations and codes in performing its obligations hereunder, including the procurement of licenses, permits and certificates and payment of taxes where required. The Successful bidder shall maintain all proper records, particularly but without limitation accounting records, required by any law, code, practice or corporate policy applicable to it from time to time including records, returns and applicable documents under the Labour Legislation 14.8 Digital Personal Data Protection Compliance The successful bidder shall comply with all applicable provisions of the Digital Personal Data Protection Act, 2023 and any rules, regulations, or guidelines issued thereunder while collecting, processing, storing, or handling any personal data in connection with this Agreement. The Successful bidder shall implement appropriate technical and organizational security measures to ensure protection of personal data against unauthorized access, disclosure, alteration, or loss. The successful bidder shall immediately notify the Bank of any actual or suspected data breach involving personal data. The successful bidder shall ensure that personal data is used solely for the	Please share a copy of the data-processing schedule covering controller/processor roles, subprocessors, processing locations, retention, deletion, breach notification timeline, audit rights and assistance obligations.	No Change, Please be guided by the RFP
736	161	14.8 / DPDP	Breach Notification	14.8 Digital Personal Data Protection Compliance The successful bidder shall comply with all applicable provisions of the Digital Personal Data Protection Act, 2023 and any rules, regulations, or guidelines issued thereunder while collecting, processing, storing, or handling any personal data in connection with this Agreement. The Successful bidder shall implement appropriate technical and organizational security measures to ensure protection of personal data against unauthorized access, disclosure, alteration, or loss. The successful bidder shall immediately notify the Bank of any actual or suspected data breach involving personal data. The successful bidder shall ensure that personal data is used solely for the purposes of performance of the contract and shall not disclose the same to any third party without prior written consent of the Bank. The successful bidder shall indemnify and hold the Bank harmless against any loss, liability, penalty, or damage arising out of any breach or non-compliance with the Digital Personal Data Protection Act, 2023. 1. The successful bidder shall assist the Bank in complying with obligations relating to Data Principal Rights such as access, correction, erasure of data, and grievance redressal under the Act. 2. The successful bidder shall not engage any sub-	Please specify a maximum contractual notification period, such as within 6 hours of confirmed awareness of a material incident, with rolling updates until containment and RCA.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
737	159	14.1 / Subcontracting	Subcontracting	14 TERMS AND CONDITIONS 14.1 Assignment & Subcontracting 1. The selected bidder shall not subcontract/JV/Consortium or permit anyone to perform any of the work, service or other performance required under the contract (excluding Proposed OEM personnels). All bidder's personnel proposed for the bank shall be on bidder's Payroll. Bank will seek relevant documentation from the bidder to validate the same. 2. If the Bank undergoes a merger, amalgamation, takeover, consolidation, reconstruction, change of ownership, etc., this tender shall be assigned to the new entity, and such an act shall not affect the rights of the Agency under this tender.	Please clarify treatment of CSPs, distributors, managed service platforms and specialized service providers, and require Bank approval plus full flow-down obligations for every material third-party dependency.	No Change, Please be guided by the RFP
738	159	14.2 / Quantity Variation	25% Variation	The Bidder/Vendor shall be bound to accept such variation and execute the order at the same rates and on the same terms and conditions as agreed under the contract. 14.2 Right to Alter quantities The bank reserves the right, at the time of award of contract and/or during the currency of the contract, to increase or decrease the quantity of goods, licenses, subscriptions, appliances, equipment, services, implementation effort, support services, or any line item covered under the contract by up to twenty-five percent (25%) of the quantities specified in the RFP/Contract, without any change in the unit prices, terms and conditions, technical specifications, delivery schedule, warranty obligations, support commitments, or any other contractual conditions.	Please clarify that any increase in cloud consumption, log retention, EPS, endpoint count or service scope that changes underlying OEM/CSP pricing metrics will be subject to corresponding agreed unit rates and technical feasibility.	No Change, Please be guided by the RFP
739	147	13 SLA	Penalty Cap	• Availability Service Levels shall be measured and evaluated on a monthly basis. • The bidder's performance against the prescribed Availability Service Levels shall be assessed monthly for each applicable solution, service, appliance, software component, or system covered under the scope of this RFP, in accordance with the minimum service levels specified in the Availability Measurement Table. • An Availability Service Level Default shall be deemed to have occurred if the bidder fails to achieve the prescribed Minimum Availability Service Level for any applicable service, solution, or component during a given month. • Availability measurements and corresponding SLA compliance assessments shall be based on the monthly performance reports and downtime records validated by the Bank. Services SLAs: Service Area Service Level Penalty Each Proposed Services Uptimes 99.90% For every 0.05% or part thereof drop in service levels penalty will be 1% of the Monthly Maintenance Cost Service level drop below 90%, penalty shall amount to 100% of the Monthly Maintenance Cost	Please confirm that all SLA/service credits, LDs and other performance penalties under the RFP are collectively capped at 10% of the total contract value, except for any explicitly stated exclusions, if applicable.	No Change, Please be guided by the RFP RFP Clause 13.2 - For the purpose of this RFP, the total penalties as per LD & SLA will be subject to a maximum of 10% of the overall contract value
740	145-151	13 SLA / Service Levels	SLA Measurement and Penalties	Availability Measurements Level Type of Measurement Minimum Service Level Penalty Infrastructure Cyber Security Proposed Availability of 99.90% For every 0.05% or part thereof drop in service levels penalty Solutions and IT Infrastructure each will be 1% of the Monthly Maintenance Cost Infrastructure & Systems solution, (HCI/Virtualization, Infrastructure OS, DB, IT Elements & Components Etc.) Systems, any	Please clarify the hierarchy and non-duplication mechanism where the same incident results in both availability downtime and incident-resolution SLA breach. Please confirm that the same event will not attract duplicate penalties under multiple SLA clauses.	No Change, Please be guided by the RFP
741	143	13 SLA / RCA	OEM RCA Requirement	The bidder shall classify, respond to, and resolve incidents in accordance with the following severity levels and associated Service Level requirements Level Classifications Criticality Table Severity Classification Criteria Response Time Resolution Time Level Critical / Any incident resulting in one or more of the following: Within 15 minutes Within 45 Minutes High 1. Complete or significant disruption preventing users from (24x7x365) performing their business operations. 2. Failure of any production component of the proposed solution, IT infrastructure, or associated services. 3. Security incidents affecting confidentiality, integrity, or availability of systems or data. 4. No acceptable workaround or manual process is available. 5. Potential financial, regulatory, operational, or reputational impact on the Bank. 6. Failure or unavailability of critical infrastructure components including, but not limited to: i. Application servers ii. Web servers iii. Database servers/appliances iv. Solution servers/appliances v. Storage vi. Backup Infrastructures vii. Network components supplied under the contract Key / Any incident resulting in one or more of the following: Within 15 minutes Within 90 Minutes Medium 1. An incident not classified as Critical, for which a temporary	Please clarify whether the RCA timeline begins after restoration of service or after closure of the incident by the Bank, and whether RCA delays caused by third-party OEM/CSP dependency will be treated as bidder-attributable delay.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
742	142-143	13 SLA / Incident Management	Four-Hour Component Restoration	The bidder shall classify, respond to, and resolve incidents in accordance with the following severity levels and associated Service Level requirements Level Classifications Criticality Table Severity Classification Criteria Response Time Resolution Time Level Critical / Any incident resulting in one or more of the following: Within 15 minutes Within 45 Minutes High 1. Complete or significant disruption preventing users from (24x7x365) performing their business operations. 2. Failure of any production component of the proposed solution, IT infrastructure, or associated services. 3. Security incidents affecting confidentiality, integrity, or availability of systems or data. 4. No acceptable workaround or manual process is available. 5. Potential financial, regulatory, operational, or reputational impact on the Bank. 6. Failure or unavailability of critical infrastructure components including, but not limited to: i. Application servers ii. Web servers iii. Database servers/appliances iv. Solution servers/appliances v. Storage vi. Backup Infrastructures vii. Network components supplied under the contract Key / Any incident resulting in one or more of the following: Within 15 minutes Within 90 Minutes Medium 1. An incident not classified as Critical, for which a temporary	Please clarify whether the four-hour requirement is measured from incident logging/notification or from technical confirmation of component failure, and whether the requirement applies equally to cloud/SaaS services where the underlying infrastructure is controlled by the CSP/OEM.	No Change, Please be guided by the RFP
743	142	13.1 / RCA	RCA Penalty	systems, firmware, BIOS, security, and related updates or patches during the contract period at no additional cost to the Bank. 16. If any customer-facing application, Core Banking System (CBS), regulatory application, statutory application, or other critical banking service becomes unavailable, disrupted, or degraded due to an issue attributable to the Core Firewall or Perimeter Firewall or solution(s) supplied under this RFP, and the incident is classified by the Bank as a Critical- Level Incident, the Bank may impose an additional penalty over and above the standard SLA penalties. Where such an incident remains unresolved for more than 120 minutes, an additional penalty of 0.5% of the monthly maintenance charges shall be levied for every subsequent hour or part thereof until the issue is resolved and normal services are restored. 17. For all incidents related to the supplied solution, the bidder shall submit a Root Cause Analysis (RCA) report issued by the respective OEM within three (3) working days from the date of incident resolution. A penalty of ₹20,000 per calendar day shall be levied for any delay in submission of the RCA report beyond the defined timelines. 18. Total penalties due Service level and liquidated damages shall not exceed 10% of the Total contract value	Please clarify that the RCA SLA starts after service restoration and that delay attributable to unavailable third-party evidence will be handled through a documented dependency exception process.	No Change, Please be guided by the RFP
744	140	12.5 Facility Management (FM) Cost	FM Manpower Cost	FM Manpower Cost: Submission of SLA report and Submission of attendance record/register of Onsite resources on Quarterly basis. Quarterly in arrears.	Please consider monthly payment in arrears for FM manpower rather than quarterly in arrears, based on validated attendance and SLA reports. Monthly billing would align payment with recurring salary and statutory employment obligations incurred by the bidder.	No Change, Please be guided by the RFP
745	140	12.6 Other Cost	Other Cost	Other Cost: Payable in arrears After completion of respective activity.	Please clarify that where an activity is completed and accepted in phases, the bidder may raise proportionate milestone invoices for each accepted phase rather than waiting for completion of the entire activity.	No Change, Please be guided by the RFP
746	140	12 PAYMENT TERMS	Payment Disputes	The selected Bidder will have to submit the documents (Delivery challans with all the part codes of OEM which shall be reconciled with BOM) at the Bank's office along with a request letter for payment. No advance payment will be made. Payment will be made in Indian Rupees only. All taxes to be paid will be subject to GST applicability. TDS will be applicable. All out of pocket expenses, travelling, boarding and lodging expenses for the entire term of this RFP and subsequent agreement is included in the amount and service provider shall not be entitled to charge any additional cost on account of any items or services or by way of any out-of-pocket expense, including travelling, boarding, and lodging etc. Bank will release payment within 30 days from the date of receipt of invoice. In case of dispute, payment will be made within 30 working days of the resolution of disputes.	Please provide that only the genuinely disputed portion of an invoice may be withheld, while the undisputed portion shall be paid within the prescribed payment cycle. This will prevent working-capital impact from disputes relating to a limited component of a consolidated invoice.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
747	140	12 PAYMENT TERMS	Invoice Acceptance	The selected Bidder will have to submit the documents (Delivery challans with all the part codes of OEM which shall be reconciled with BOM) at the Bank's office along with a request letter for payment. No advance payment will be made. Payment will be made in Indian Rupees only. All taxes to be paid will be subject to GST applicability. TDS will be applicable. All out of pocket expenses, travelling, boarding and lodging expenses for the entire term of this RFP and subsequent agreement is included in the amount and service provider shall not be entitled to charge any additional cost on account of any items or services or by way of any out-of-pocket expense, including travelling, boarding, and lodging etc. Bank will release payment within 30 days from the date of receipt of invoice. In case of dispute, payment will be made within 30 working days of the resolution of disputes.	Please establish an invoice validation/acceptance workflow with a defined timeline, including deemed acceptance where the Bank does not raise a specific written objection within 7 working days. This will provide predictable receivables and reduce open-ended invoice ageing.	No Change, Please be guided by the RFP
748	140	12 PAYMENT TERMS	Interest on Delayed Payment	The selected Bidder will have to submit the documents (Delivery challans with all the part codes of OEM which shall be reconciled with BOM) at the Bank's office along with a request letter for payment. No advance payment will be made. Payment will be made in Indian Rupees only. All taxes to be paid will be subject to GST applicability. TDS will be applicable. All out of pocket expenses, travelling, boarding and lodging expenses for the entire term of this RFP and subsequent agreement is included in the amount and service provider shall not be entitled to charge any additional cost on account of any items or services or by way of any out-of-pocket expense, including travelling, boarding, and lodging etc. Bank will release payment within 30 days from the date of receipt of invoice. In case of dispute, payment will be made within 30 working days of the resolution of disputes.	Please consider inclusion of a reasonable interest mechanism for payments delayed beyond the contractual payment period for reasons not attributable to the bidder, subject to applicable Bank/GeM rules. This would provide a balanced commercial framework and discourage prolonged receivable ageing.	No Change, Please be guided by the RFP
749	139-140	12.4 ATS/Subscription/AMC	Annual Subscription / ATS / AMC	The Bidder is required to submit the required to submit the following: • Delivery proof • OOTB Installation Proof • Invoice of the Product On successful UAT Signoff of the respective product 20% On successful Go-live of the respective product 30% Delivery of hardware and submission of invoice with 70% Proof of Delivery and other documents of the hardware supplied. Bank may at its discretion verify the details before releasing the payment Hardware (This verification, if required, shall be completed within 1 Cost (Other 2. month of delivery of the hardware on the bank's than premises). Appliances) On successful installation of proposed solutions on the 15% hardware - 50% of the sought product/solutions On successful installation of remaining proposed solution 15% on the hardware – remaining 50% of the sought product/solutions OOTB – Out of the Box (The features marked as standard feature by the OEMs of the respective solution in the compliance sheets) 12.4 ATS/subscription cost & AMC Cost (ATS/ subscription cost & AMC Cost – Annual ATS & AMC Support of the respective software & hardware) S. No Items Milestone Percentage 1 ATS/ Annual ATS/ Annual Annually in Advance: Upon submission of a Subscription & Subscription Bank Guarantee	Please confirm whether the bidder may choose either payment option for each OEM solution independently, and whether the 110% Bank Guarantee is required for the entire annual amount including applicable taxes or only the pre-tax annual subscription/ATS amount.	No Change, Please be guided by the RFP
750	139-140	12.4 ATS/subscription cost & AMC Cost	110% Bank Guarantee	ATS/ Annual Subscription & Appliance AMC Cost: ATS/ Annual Subscription Cost Annually in Advance: Upon submission of a Bank Guarantee equivalent to 110% of the annual subscription/Annual technical cost of the respective product, valid for the applicable subscription period; or Quarterly in Arrears. Appliance AMC Annually in advance, upon submission of a Bank Guarantee equivalent to 110% of the annual AMC amount of the respective product, or quarterly in arrears, as per the terms and conditions of the Contract.	Where the Bank retains the annual-in-advance option, please consider reducing the Bank Guarantee requirement from 110% to 100% of the applicable annual amount and allowing the BG to reduce proportionately as the subscription/service period is consumed.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
751	139	12.3 Hardware Cost	Appliance Cost	Appliance Cost: On successful Delivery of the Appliance which would be considered delivered once the solution (with OOTB features) is made available for view and review of the bank. The Bidder is required to submit the following: Delivery proof; OOTB Installation Proof; Invoice of the Product 50%. On successful UAT Signoff of the respective product 20%. On successful Go-live of the respective product 30%. Hardware Cost (Other than Appliances): Delivery of hardware and submission of invoice with Proof of Delivery and other documents of the hardware supplied. Bank may at its discretion verify the details before releasing the payment (This verification, if required, shall be completed within 1 month of delivery of the hardware on the bank's premises). 70%. On successful installation of proposed solutions on the hardware - 50% of the sought product/solutions 15%. On successful installation of remaining proposed solution on the hardware – remaining 50% of the sought product/solutions 15%.	Please consider increasing the appliance delivery milestone from 50% to 70%, with 15% at UAT and 15% at Go-Live, since the bidder incurs the OEM/appliance procurement cost substantially before UAT and Go-Live.	No Change, Please be guided by the RFP
752	139	12.3 Hardware Cost	Hardware Cost (Other than Appliances)	Appliance Cost: On successful Delivery of the Appliance which would be considered delivered once the solution (with OOTB features) is made available for view and review of the bank. The Bidder is required to submit the following: Delivery proof; OOTB Installation Proof; Invoice of the Product 50%. On successful UAT Signoff of the respective product 20%. On successful Go-live of the respective product 30%. Hardware Cost (Other than Appliances): Delivery of hardware and submission of invoice with Proof of Delivery and other documents of the hardware supplied. Bank may at its discretion verify the details before releasing the payment (This verification, if required, shall be completed within 1 month of delivery of the hardware on the bank's premises). 70%. On successful installation of proposed solutions on the hardware - 50% of the sought product/solutions 15%. On successful installation of remaining proposed solution on the hardware – remaining 50% of the sought product/solutions 15%.	Please consider permitting 80% payment upon delivery and verification of hardware, with the remaining 20% linked to installation/commissioning, since the bidder incurs the majority of hardware procurement and logistics cost before installation.	No Change, Please be guided by the RFP
753	139	12.3 Hardware Cost	Hardware Verification	Appliance Cost: On successful Delivery of the Appliance which would be considered delivered once the solution (with OOTB features) is made available for view and review of the bank. The Bidder is required to submit the following: Delivery proof; OOTB Installation Proof; Invoice of the Product 50%. On successful UAT Signoff of the respective product 20%. On successful Go-live of the respective product 30%. Hardware Cost (Other than Appliances): Delivery of hardware and submission of invoice with Proof of Delivery and other documents of the hardware supplied. Bank may at its discretion verify the details before releasing the payment (This verification, if required, shall be completed within 1 month of delivery of the hardware on the bank's premises). 70%. On successful installation of proposed solutions on the hardware - 50% of the sought product/solutions 15%. On successful installation of remaining proposed solution on the hardware – remaining 50% of the sought product/solutions 15%.	The RFP permits Bank verification of hardware details for up to one month after delivery. Please confirm that where no discrepancy is notified within 7 working days of delivery, the delivery milestone shall be deemed accepted and invoiced for payment, subject to reconciliation of OEM part codes and required documents.	No Change, Please be guided by the RFP
754	138-139	12 PAYMENT TERMS	Product / Implementation Payment	12.3 Hardware Cost (Hardware cost is defined as the sum of One time Hardware Cost, and Installation cost of the respective hardware) S. Milestone Percentage Items No. On successful Delivery of the Appliance which would be 50% Appliance 1 considered delivered once the solution (with OOTB Cost features) is made available for view and review of the bank.	Please clarify whether 'delivery' for Cloud/SaaS subscriptions will be deemed achieved upon activation/provisioning of the tenant and access credentials, rather than physical delivery, and whether the same milestone treatment applies uniformly to all SaaS solutions.	No Change, Please be guided by the RFP
755	138-139	12.2 OEM Services Cost	OEM Services Cost	OEM Services Cost Payable in arrears post providing the service. Quarterly in arrears. Architecture Assessment: Submission of Report to Bank along with detailed presentation to bank's senior management on yearly basis. In arrears. Payment will begin after sign-off of the services configurations and the bank has started using the same for its intended use.	Please consider monthly invoicing in arrears for OEM services instead of quarterly in arrears, particularly where OEM resources and specialist services are deployed continuously. This would materially reduce the bidder's working-capital cycle without increasing the Bank's overall contractual cost.	No Change, Please be guided by the RFP
756	138-139	12.2 OEM Services Cost	Architecture Assessment	OEM Services Cost Payable in arrears post providing the service. Quarterly in arrears. Architecture Assessment: Submission of Report to Bank along with detailed presentation to bank's senior management on yearly basis. In arrears. Payment will begin after sign-off of the services configurations and the bank has started using the same for its intended use.	For annual Architecture Assessment services, please permit payment upon submission and Bank acceptance of the annual assessment report and presentation, rather than linking payment to other service configuration sign-offs.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
757	138	12.1 Product (Software) Cost	Subscription Cost	Subscription Cost (One time license Cost): On successful delivery of the Licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware. The Bidder is required to submit the following: Delivery proof; OOTB Installation Proof; Invoice of the Product 50%. On successful UAT Signoff of the respective product 20%. On successful Go-live of the respective product 30%.	Please consider below Payment Terms: Subscription Cost (One time license Cost): On successful delivery of the Licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware. The Bidder is required to submit the following: Delivery proof; OOTB Installation Proof; Invoice of the Product 70%. On successful UAT Signoff of the respective product 15%. On successful Go-live of the respective product 15%.	No Change, Please be guided by the RFP
758	137-140	12 PAYMENT TERMS	Milestone Acceptance Independence	Note: a. Annual Maintenance Contract (AMC)/ Annual Technical Support (ATS) includes all appliance, software, applications, component, services deployed/required to meet the required terms of the RFP. b. Activities need to be carried out simultaneously for speedy production roll out as per Bank's expectations and standards. Bank may involve third parties at various stages for review, verification of completeness of NextGEN SOC Security setup and onsite & offsite activities etc. without obtaining permission from the bidder & OEMs.	Please confirm that payment for a successfully delivered and accepted product/service will not be withheld because another unrelated OEM/product/workstream has pending acceptance, subject to the accepted item meeting its own contractual requirements.	No Change, Please be guided by the RFP
759	137-140	12 PAYMENT TERMS	Mobilization Costs	The selected Bidder will have to submit the documents (Delivery challans with all the part codes of OEM which shall be reconciled with BOM) at the Bank's office along with a request letter for payment. No advance payment will be made. Payment will be made in Indian Rupees only. All taxes to be paid will be subject to GST applicability. TDS will be applicable. All out of pocket expenses, travelling, boarding and lodging expenses for the entire term of this RFP and subsequent agreement is included in the amount and service provider shall not be entitled to charge any additional cost on account of any items or services or by way of any out-of-pocket expense, including travelling, boarding, and lodging etc. Bank will release payment within 30 days from the date of receipt of invoice. In case of dispute, payment will be made within 30 working days of the resolution of disputes.	Please consider a mobilization milestone payable upon completion of project kick-off, resource onboarding, project-plan approval and OEM mobilization, against appropriate documentary evidence. This would recognize the substantial upfront manpower and mobilization costs incurred before product delivery/UAT.	No Change, Please be guided by the RFP
760	137-140	12 PAYMENT TERMS	Payment and Scope Variation	The selected Bidder will have to submit the documents (Delivery challans with all the part codes of OEM which shall be reconciled with BOM) at the Bank's office along with a request letter for payment. No advance payment will be made. Payment will be made in Indian Rupees only. All taxes to be paid will be subject to GST applicability. TDS will be applicable. All out of pocket expenses, travelling, boarding and lodging expenses for the entire term of this RFP and subsequent agreement is included in the amount and service provider shall not be entitled to charge any additional cost on account of any items or services or by way of any out-of-pocket expense, including travelling, boarding, and lodging etc. Bank will release payment within 30 days from the date of receipt of invoice. In case of dispute, payment will be made within 30 working days of the resolution of disputes.	Where the Bank exercises its right to increase quantities or procure additional services, please confirm the payment structure and timelines.	Please refer to Section 14.2 and Section 12 of the RFP.
761	137-140	12 PAYMENT TERMS	Payment for Additional Capacity	The selected Bidder will have to submit the documents (Delivery challans with all the part codes of OEM which shall be reconciled with BOM) at the Bank's office along with a request letter for payment. No advance payment will be made. Payment will be made in Indian Rupees only. All taxes to be paid will be subject to GST applicability. TDS will be applicable. All out of pocket expenses, travelling, boarding and lodging expenses for the entire term of this RFP and subsequent agreement is included in the amount and service provider shall not be entitled to charge any additional cost on account of any items or services or by way of any out-of-pocket expense, including travelling, boarding, and lodging etc. Bank will release payment within 30 days from the date of receipt of invoice. In case of dispute, payment will be made within 30 working days of the resolution of disputes.	Where additional SIEM capacity, storage, licenses, infrastructure or manpower is required during the contract, please confirm that the corresponding additional quantities will be invoiced and paid upon delivery/activation.	Please refer to Section 14.2 and Section 12 of the RFP.
762	137-138	12.1 Product (Software) Cost	Product License Cost	Product Cost is defined as the sum of One time Product License Cost and One time implementation cost of the respective product. Product License Cost: On successful delivery of the licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware. The Bidder is required to submit the following: Delivery proof; OOTB Installation Proof; Invoice of the Product. 50%. On successful UAT Signoff of the respective product 20%. On successful Go-live of the respective product 30%.	Please consider increasing the payment linked to delivery of software licenses from 50% to 70%, with 15% on UAT and 15% on Go-Live, since the bidder incurs the OEM license/subscription commitment at the time of procurement. Alternatively, permit milestone-based payment immediately upon OEM license activation/entitlement.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
763	137-138	12.1 Product (Software) Cost	Product Implementation Cost	Product Implementation Cost: On Successful installation of OOTB product on the sourced hardware and handing over the environment with OOTB product to Bank 20%. On successful UAT Signoff of the respective product 50%. On successful Go-live of the respective product 20%. Within 3 months of successful Go-live 10%.	Please consider revising the implementation milestone from 20% installation / 50% UAT / 20% Go-Live / 10% post-Go-Live to 30% installation / 40% UAT / 20% Go-Live / 10% post-Go-Live, thereby better aligning payment with actual implementation effort and resource deployment.	No Change, Please be guided by the RFP
764	137-138	12.1 Product (Software) Cost	Post-Go-Live Holdback	Product Implementation Cost: On Successful installation of OOTB product on the sourced hardware and handing over the environment with OOTB product to Bank 20%. On successful UAT Signoff of the respective product 50%. On successful Go-live of the respective product 20%. Within 3 months of successful Go-live 10%.	Please consider reducing the 10% payment held for three months after Go-Live to 5%, with the balance 5% released at Go-Live subject to successful acceptance, as the bidder has already incurred OEM, manpower and implementation costs well before the three-month period.	No Change, Please be guided by the RFP
765	137-138	12.1 Product (Software) Cost	UAT Dependency	Product Cost is defined as the sum of One time Product License Cost and One time implementation cost of the respective product. Product License Cost: On successful delivery of the licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware. The Bidder is required to submit the following: Delivery proof; OOTB Installation Proof; Invoice of the Product. 50%. On successful UAT Signoff of the respective product 20%. On successful Go-live of the respective product 30%.	Please define a maximum timeline for Bank UAT and sign-off, such as 10 working days from submission of the UAT-ready solution. Where the Bank does not provide observations within that period, may the milestone be deemed accepted for payment purposes, subject to the contractual acceptance criteria?	No Change, Please be guided by the RFP
766	137-138	12.1 Product (Software) Cost	Partial Acceptance	Product Cost is defined as the sum of One time Product License Cost and One time implementation cost of the respective product. Product License Cost: On successful delivery of the licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware. The Bidder is required to submit the following: Delivery proof; OOTB Installation Proof; Invoice of the Product. 50%. On successful UAT Signoff of the respective product 20%. On successful Go-live of the respective product 30%.	As the RFP contains multiple products and OEMs, please permit milestone-wise and solution-wise invoicing/payment for each independently completed and accepted solution rather than linking payment for one solution to completion of unrelated solutions.	No Change, Please be guided by the RFP
767	137	12 PAYMENT TERMS	General Payment Terms	The selected Bidder will have to submit the documents (Delivery challans with all the part codes of OEM which shall be reconciled with BOM) at the Bank's office along with a request letter for payment. No advance payment will be made. Payment will be made in Indian Rupees only. All taxes to be paid will be subject to GST applicability. TDS will be applicable. All out of pocket expenses, travelling, boarding and lodging expenses for the entire term of this RFP and subsequent agreement is included in the amount and service provider shall not be entitled to charge any additional cost on account of any items or services or by way of any out-of-pocket expense, including travelling, boarding, and lodging etc. Bank will release payment within 30 days from the date of receipt of invoice. In case of dispute, payment will be made within 30 working days of the resolution of disputes.	Please consider revising the payment terms to provide a defined maximum payment cycle of 30 calendar days from receipt of a complete and undisputed invoice, with the invoice being deemed accepted unless rejected with specific reasons within 7 working days. This will provide greater predictability of cash flows and reduce working-capital exposure over the 5-month implementation and subsequent O&M period.	No Change, Please be guided by the RFP
768	137	12 PAYMENT TERMS	No Advance Payment	The selected Bidder will have to submit the documents (Delivery challans with all the part codes of OEM which shall be reconciled with BOM) at the Bank's office along with a request letter for payment. No advance payment will be made. Payment will be made in Indian Rupees only. All taxes to be paid will be subject to GST applicability. TDS will be applicable. All out of pocket expenses, travelling, boarding and lodging expenses for the entire term of this RFP and subsequent agreement is included in the amount and service provider shall not be entitled to charge any additional cost on account of any items or services or by way of any out-of-pocket expense, including travelling, boarding, and lodging etc. Bank will release payment within 30 days from the date of receipt of invoice. In case of dispute, payment will be made within 30 working days of the resolution of disputes.	Considering that the bidder must procure OEM licenses, hardware, subscriptions and implementation resources upfront, please consider permitting a reasonable mobilization/advance payment, e.g. 10% of the implementation/product value, against an equivalent Advance Bank Guarantee, subject to applicable Bank/GeM rules. This would reduce substantial upfront working-capital funding by the bidder.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
769	129-136	10.3-10.4 / Evaluation	QCBS	10.4 Commercial Evaluation Criteria The commercial bid of only Eligible & technically qualified bidders shall be opened. These qualified bidders as per evaluation process will participate in Commercial evaluation process. The Commercial offers of only those Bidders, who are short-listed after technical evaluation, would be opened. The format for quoting commercial bid is set in Appendix 2-Commercial Bill of Material. The commercial offer should consist of comprehensive cost for required solution. The bidder must provide detailed cost breakdown, for each category mentioned in the commercial bid. The Bank reserves the right to proceed with the commercial bid opening and subsequent procurement process even if only one bidder qualifies the eligibility evaluation criteria stipulated under this RFP. Such a decision may be taken by the Bank at its sole discretion, considering the criticality of the requirement, urgency of implementation, business continuity needs, operational considerations, or any other factors deemed relevant by the Bank. The decision of the Bank in this regard shall be final, conclusive, and binding on all bidders. The commercial offer should consist of comprehensive cost for all the components in the format provided in Appendix 2: Commercial Bill of Material Bidder must	Please consider adopting QCBS, e.g. 70% technical/quality and 30% commercial, because the engagement is a strategic, multi-OEM, technology-intensive managed cybersecurity transformation where lowest price alone may not represent lowest risk or best value.	No Change, Please be guided by the RFP
770	129-136	10.3 / Technical Evaluation	Technical Threshold	10.3 Technical Evaluation Criteria Only those bidders who are found to be responsive and who meet all the Pre-Qualification (PQ) (Section 10.2) Criteria of the RFP, as determined by the Bank, shall be evaluation for technical Evaluation Criteria (Section 10.3). Bidder must score minimum 80% overall technical score (80/100 marks). Marks obtained by the bidder under each line item of table will be normalized to their weightages as shown in the table summing to a total of 100 Commercial Price Bids will only be opened for bidders who qualify the minimum technical qualification criteria as detailed below	Please increase the overall technical qualifying threshold to at least 85/100 and introduce mandatory minimum section scores for architecture, SOC operations, implementation, resilience and security.	No Change, Please be guided by the RFP
771	129-136	10.3 / Technical Evaluation	Solution-Level Threshold	10.4 Commercial Evaluation Criteria The commercial bid of only Eligible & technically qualified bidders shall be opened. These qualified bidders as per evaluation process will participate in Commercial evaluation process. The Commercial offers of only those Bidders, who are short-listed after technical evaluation, would be opened. The format for quoting commercial bid is set in Appendix 2-Commercial Bill of Material. The commercial offer should consist of comprehensive cost for required solution. The bidder must provide detailed cost breakdown, for each category mentioned in the commercial bid. The Bank reserves the right to proceed with the commercial bid opening and subsequent procurement process even if only one bidder qualifies the eligibility evaluation criteria stipulated under this RFP. Such a decision may be taken by the Bank at its sole discretion, considering the criticality of the requirement, urgency of implementation, business continuity needs, operational considerations, or any other factors deemed relevant by the Bank. The decision of the Bank in this regard shall be final, conclusive, and binding on all bidders. The commercial offer should consist of comprehensive cost for all the components in the format provided in Appendix 2: Commercial Bill of Material Bidder must	Please introduce minimum technical scores for each critical solution such as SIEM/SOAR/UEBA solutions.	No Change, Please be guided by the RFP
772	129-136	10.3 / Technical Evaluation	Architecture Score	10.3 Technical Evaluation Criteria Only those bidders who are found to be responsive and who meet all the Pre-Qualification (PQ) (Section 10.2) Criteria of the RFP, as determined by the Bank, shall be evaluation for technical Evaluation Criteria (Section 10.3). Bidder must score minimum 80% overall technical score (80/100 marks). Marks obtained by the bidder under each line item of table will be normalized to their weightages as shown in the table summing to a total of 100	Please allocate a dedicated technical weight to architecture and resilience, including HA, DC/DR, cloud security, integration, scalability, zero-trust administration and operational continuity.	No Change, Please be guided by the RFP
773	129-136	10.3 / Technical Evaluation	SOC Operating Model	S.No. Criteria Scoring 4. Phishing simulation 5. Anti-phishing services 6. Dark web monitoring 7. Brand protection & monitoring 8. Threat Intelligence feed 9. Threat Hunting services Category: a. Point 1: 1 Client b. Point 2: >2 Clients 7 Technical presentation Max Marks 10 A presentation to be made by the bidder covering the following aspects (but not limited to): a. Capability demonstration by the bidder b. Understanding of Scope of work & terms of the RFP c. Proposed Approach and Methodology for implementation d. Approach & methodology for providing Managed Security Services (MSS) to run Security Operation Centre (SOC) services e. Solution Description, Functionality, Architecture & Deployment model, Posture of proposed architecture f. Resource Deployment plan, Implementation Plan g. OEM Proposed project detailed Go-Live timelines for each solution with milestones. h. Bidder to demonstrate a relevant AI/ML capability use case, playbooks, models etc.	Please allocate a dedicated score to SOC operating maturity covering L1/L2/L3 model, detection engineering, threat hunting, IR, automation, QA, governance and continual improvement.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
774	129-136	10.3 / Technical Evaluation	Cyber Resilience	The Bank reserves the right, at its sole discretion and in the interest of economy, optimization of requirements, technological suitability, or business/operational necessity, to accept, reject, reduce, modify, defer, or descope - one or more Solution Components, Modules, Licences, Services, Quantities, or associated IT Infrastructure items forming part of the scope of this RFP, at any stage prior to issuance of the Contract/Letter of Award. The commercial bid shall be evaluated on the basis of the originally specified scope and quantities as published in the RFP/GeM bid.	Please allocate a dedicated score for cyber resilience covering recovery architecture, ransomware resilience, immutable backup, DR testing, crisis management and recovery validation.	No Change, Please be guided by the RFP
775	129-136	10.3 / Technical Evaluation	AI/ML	S.No. Criteria Scoring provider, with demonstrated deployment experience meeting the Max Marks – 15 Marks following:	Please score AI/ML on measurable production capability, explainability, model governance, automation outcomes and analyst augmentation rather than marketing claims.	No Change, Please be guided by the RFP
776	129-136	10.3 / Technical Evaluation	OEM Strength	S.No. Criteria Scoring Even if the installation was completed more than five years ago, it will still qualify, provided the bidder is currently maintaining that solution or has carried out its maintenance at any time during the five-year period preceding the RFP publication date 4 The proposed OEM solution (solution list in mentioned below) should Point 1 = 2 Marks have been implemented in Client (BFSI/PSU/PSE/ Govt Organization) Point 2 = 3 Marks in India. Max Marks – 30 Marks Bidder to substantiate the clause for each of the below-mentioned solution and scoring for each of the solution would be summed to arrive at the solution OEM experience score. List of Solutions are: 1. SOAR 2. UEBA 3. Extended detection & response (XDR) 4. Network detection & response (NDR) 5. Decoy/HoneyPot/Deception 6. Threat Intelligence Platform 7. Vulnerability Assessment/Vulnerability Management 8. Identity Theft Detection & response 9. Application Security testing Tool (Both DAST & SAST) 10. Cloud Security posture Management tool (CSPM)	Please require evidence of current India support organization, named SMEs, product roadmap, escalation capability and local engineering presence for each critical OEM.	No Change, Please be guided by the RFP
777	129-136	10.3 / Technical Evaluation	Reference Quality	Bank reserves the right to perform the reference check through VC/Reference call/site visit/other mode of communication as deemed necessary by the evaluation team.	Please weight reference quality by relevance, scale, duration, current operational status, BFSI/regulatory similarity and integration complexity rather than client count alone.	No Change, Please be guided by the RFP
778	129-136	10.3 / Technical Evaluation	Scale Experience	S.No. Criteria Scoring provider, with demonstrated deployment experience meeting the Max Marks – 15 Marks following: 1. Point 1: 20000 EPS / 0.86 TB per day ≤ SIEM Solution Experience < 25,000 EPS / 1.00 TB per day 2. Point 2: 25,000 EPS / 1.00 TB per day ≤ SIEM Solution Experience < 30,000 EPS / 1.20 TB per day 3. Point 3: 30,000 EPS / 1.20 TB per day ≤ SIEM Solution Experience OEM Evaluation Criteria 3 The proposed OEM SIEM solution should have been implemented (and Point 1 = 3 Marks should be maintained/under-maintenance) in PSU/PSE, Government Point 2 = 5 Marks Organisation, BFSI organisation/Telecom/Fortune 500 (Last 3 years) Point 3 = 5 Marks in India with the following requirement as mentioned in the below Point 4 = 10 Marks category. Point 5 = 8 Marks Category: Point 6 = 15 Marks i. Category 1: 30000 EPS/ 1.2TB per day or more a. Point 1 →Client = 1 Max Marks – 15 Marks b. Point 2 →Client = 2 ii. Category 2: 50000 EPS/ 2TB per day or more a. Point 3 →Client = 1 b. Point 4 →Client = 2 iii. Category 3: 75000 EPS/ 3TB per day or more a. Point 5 →Client = 1 b. Point 6 →Client = 2 (of which 1 should be a Scheduled Commercial Bank)	Please score sustained production scale, not only licensed capacity, and require evidence of actual observed ingestion, peak load, retention, query workload and operational uptime.	Please refer addendum for revised clause.
779	129-136	10.3 / Technical Evaluation	Multi-OEM Integration	S.No. Criteria Scoring 4. Phishing simulation 5. Anti-phishing services 6. Dark web monitoring 7. Brand protection & monitoring 8. Threat Intelligence feed 9. Threat Hunting services Category: a. Point 1: 1 Client b. Point 2: >2 Clients 7 Technical presentation Max Marks 10 A presentation to be made by the bidder covering the following aspects (but not limited to): a. Capability demonstration by the bidder b. Understanding of Scope of work & terms of the RFP c. Proposed Approach and Methodology for implementation d. Approach & methodology for providing Managed Security Services (MSS) to run Security Operation Centre (SOC) services e. Solution Description, Functionality, Architecture & Deployment model, Posture of proposed architecture f. Resource Deployment plan, Implementation Plan g. OEM Proposed project detailed Go-Live timelines for each solution with milestones. h. Bidder to demonstrate a relevant AI/ML capability use case, playbooks, models etc.	Please introduce a scoring category for demonstrated multi-technology integrations where the bidder has successfully operated heterogeneous SIEM/SOAR/UEBA/XDR/NDR/identity/cloud security stacks.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
780	129-136	10.3 / Technical Evaluation	Resource Quality	S.No. Criteria Scoring 4. Phishing simulation 5. Anti-phishing services 6. Dark web monitoring 7. Brand protection & monitoring 8. Threat Intelligence feed 9. Threat Hunting services Category: a. Point 1: 1 Client b. Point 2: >2 Clients 7 Technical presentation Max Marks 10 A presentation to be made by the bidder covering the following aspects (but not limited to): a. Capability demonstration by the bidder b. Understanding of Scope of work & terms of the RFP c. Proposed Approach and Methodology for implementation d. Approach & methodology for providing Managed Security Services (MSS) to run Security Operation Centre (SOC) services e. Solution Description, Functionality, Architecture & Deployment model, Posture of proposed architecture f. Resource Deployment plan, Implementation Plan g. OEM Proposed project detailed Go-Live timelines for each solution with milestones. h. Bidder to demonstrate a relevant AI/ML capability use case, playbooks, models etc.	Please score named key personnel on relevant certifications, years of SOC experience, BFSI references, detection-engineering skills, cloud skills and tenure with bidder, rather than headcount alone.	No Change, Please be guided by the RFP
781	129-136	10.3 / Technical Evaluation	Implementation Methodology	S.No. Criteria Scoring 4. Phishing simulation 5. Anti-phishing services 6. Dark web monitoring 7. Brand protection & monitoring 8. Threat Intelligence feed 9. Threat Hunting services Category: a. Point 1: 1 Client b. Point 2: >2 Clients 7 Technical presentation Max Marks 10 A presentation to be made by the bidder covering the following aspects (but not limited to): a. Capability demonstration by the bidder b. Understanding of Scope of work & terms of the RFP c. Proposed Approach and Methodology for implementation d. Approach & methodology for providing Managed Security Services (MSS) to run Security Operation Centre (SOC) services e. Solution Description, Functionality, Architecture & Deployment model, Posture of proposed architecture f. Resource Deployment plan, Implementation Plan g. OEM Proposed project detailed Go-Live timelines for each solution with milestones. h. Bidder to demonstrate a relevant AI/ML capability use case, playbooks, models etc.	Please require a detailed migration/cutover strategy including coexistence, rollback, log-source onboarding, detection migration, data migration, UAT, DR readiness and operational transition.	Please
782	129-136	10.3 / Technical Evaluation	Commercial Reasonableness	10.4 Commercial Evaluation Criteria The commercial bid of only Eligible & technically qualified bidders shall be opened. These qualified bidders as per evaluation process will participate in Commercial evaluation process. The Commercial offers of only those Bidders, who are short-listed after technical evaluation, would be opened. The format for quoting commercial bid is set in Appendix 2-Commercial Bill of Material. The commercial offer should consist of comprehensive cost for required solution. The bidder must provide detailed cost breakdown, for each category mentioned in the commercial bid. The Bank reserves the right to proceed with the commercial bid opening and subsequent procurement process even if only one bidder qualifies the eligibility evaluation criteria stipulated under this RFP. Such a decision may be taken by the Bank at its sole discretion, considering the criticality of the requirement, urgency of implementation, business continuity needs, operational considerations, or any other factors deemed relevant by the Bank. The decision of the Bank in this regard shall be final, conclusive, and binding on all bidders. The commercial offer should consist of comprehensive cost for all the components in the format provided in Appendix 2: Commercial Bill of Material Bidder must	If QCBS is not adopted, Bidder requsts for introduction of minimum commercial reasonableness and total-cost-risk assessment to identify materially underpriced bids that could compromise service quality or later result in change claims.	No Change, Please be guided by the RFP
783	129-136	10.3 / Technical Evaluation	Cyber Risk Quantification	S.No. Criteria Scoring 4. Phishing simulation 5. Anti-phishing services 6. Dark web monitoring 7. Brand protection & monitoring 8. Threat Intelligence feed 9. Threat Hunting services Category: a. Point 1: 1 Client b. Point 2: >2 Clients 7 Technical presentation Max Marks 10 A presentation to be made by the bidder covering the following aspects (but not limited to): a. Capability demonstration by the bidder b. Understanding of Scope of work & terms of the RFP c. Proposed Approach and Methodology for implementation d. Approach & methodology for providing Managed Security Services (MSS) to run Security Operation Centre (SOC) services e. Solution Description, Functionality, Architecture & Deployment model, Posture of proposed architecture f. Resource Deployment plan, Implementation Plan g. OEM Proposed project detailed Go-Live timelines for each solution with milestones. h. Bidder to demonstrate a relevant AI/ML capability use case, playbooks, models etc.	Please introduce a dedicated score for cyber-risk quantification capability, requiring bidders to demonstrate how technical findings from CTEM, VA, ASM, TI, identity and SOC incidents are translated into business risk and executive decision metrics.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
784	127-128	10.2 / Experience Evidence	Reference Validation	l. Experience should be during the five-year period preceding the RFP publication date. Even if the installation was completed more than five years ago, it will still qualify, provided the product is currently under maintenance or has been maintained at any time during the five-year period preceding the RFP publication date m. Experience must be showcased separately for each solution category, with clear evidence that each solution has been deployed as a standalone solution and not merely as a feature or component of another solution. n. When deemed necessary the Evaluation Committee may seek clarification on relevant aspects from the Bidder. However, that would not entitle the Bidder to change or cause any change. o. Bank reserves the right to conduct reference site visit/ video conference/ voice call with the Client to substantiate the credentials/ copy of PO/ Contract copy/ sign-off submitted by Bidder and/ or OEM. In case the input/ feedback received from the Customer is negative/ unsatisfactory, bank reserves the right to reject the Bid.	Please require bidders to provide at least three reference contacts from comparable BFSI/PSU/Government deployments and permit direct technical reference validation before final scoring.	No Change, Please be guided by the RFP
785	127-128	10.2 / Experience Evidence	Revenue Relevance	verify, evaluate, and validate the information and claims submitted by the bidder. The decision of the Bank in this regard shall be final, conclusive, and binding on the bidder. b. In the event of a business transfer, acquisition, slump sale, merger, or acquisition of a business undertaking, the work experience, credentials, and references of the transferor entity ("Seller") pertaining to the acquired business may be considered, subject to submission of documentary evidence establishing such transfer and continuity of business operations. c. In cases involving corporate restructuring, including merger, amalgamation, demerger, name change, conversion, or reorganization, the incorporation certificate, financial statements, work experience credentials, technical qualifications, and other relevant records of the predecessor entity may be considered, subject to submission of documentary evidence acceptable to the Bank. d. Either the Principal/OEM or its authorized agent may submit a bid for a given item/product under this RFP. However, both the Principal/OEM and its authorized agent shall not be permitted to submit bids simultaneously for the same item/product in the same RFP. Further, where an agent is authorized to represent a Principal/OEM, the same agent shall not submit bids on behalf of more	Please require at least one comparable managed SOC engagement with 24x7 operations, multi-platform monitoring, incident response and five-year/long-term service responsibility.	No Change, Please be guided by the RFP
786	127-128	10.2 / Experience Evidence	Prime Integrator Experience	verify, evaluate, and validate the information and claims submitted by the bidder. The decision of the Bank in this regard shall be final, conclusive, and binding on the bidder. b. In the event of a business transfer, acquisition, slump sale, merger, or acquisition of a business undertaking, the work experience, credentials, and references of the transferor entity ("Seller") pertaining to the acquired business may be considered, subject to submission of documentary evidence establishing such transfer and continuity of business operations. c. In cases involving corporate restructuring, including merger, amalgamation, demerger, name change, conversion, or reorganization, the incorporation certificate, financial statements, work experience credentials, technical qualifications, and other relevant records of the predecessor entity may be considered, subject to submission of documentary evidence acceptable to the Bank. d. Either the Principal/OEM or its authorized agent may submit a bid for a given item/product under this RFP. However, both the Principal/OEM and its authorized agent shall not be permitted to submit bids simultaneously for the same item/product in the same RFP. Further, where an agent is authorized to represent a Principal/OEM, the same agent shall not submit bids on behalf of more	Please require the prime bidder to demonstrate end-to-end responsibility for architecture, integration, migration, operations and SLA management rather than relying primarily on OEM credentials.	No Change, Please be guided by the RFP
787	123-124	10.2 / Functional Compliance	Functional Score	Functional Compliance: The Bidder's proposed solution shall be evaluated for functional compliance against the requirements specified in Appendix 1A: Functional Compliance Sheet. a) OEM Self Declaration The proposed product should have minimum functional b) Filled Appendix 1A: Functional Compliance 25. compliance score of 85% for each of the following: Supporting Documentation like datasheets, product manuals, OEM website product feature listings etc. Solution List: 1. SIEM 2. SOAR 3. UEBA	Please increase the minimum functional compliance threshold to 90% for all core platforms and 95% for SIEM, SOAR, UEBA, XDR and NDR, with all critical mandatory functions required to be compliant.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
788	110-122	10.2 / OEM Evaluation Criteria	OEM SIEM Experience	# Eligibility Criteria/Clause Documents Required 19. The proposed OEM SIEM Solution with a minimum capacity of Document 1: Copy of Purchase Order / Work Order / Contract 30,000 EPS or 1.2 TB/day shall have been successfully The submitted client-issued document shall clearly indicate, either implemented and be under management/maintenance in at least directly or through a combination of documents forming part of the one (1) BFSI in India. same contract: a. Name of the Client. and b. Date of Issue/Signing. c. Scope of Work. The proposed OEM SIEM Solution with a minimum capacity of d. Solution Name and OEM Name 30,000 EPS or 1.2 TB/day shall have been successfully e. SIEM Capacity, clearly indicating one of the following, as implemented on cloud in one (1) in India. applicable: a. Minimum 30,000 EPS or 1.2 TB/day. Note: - OR A bidder's experience in supplying and installing a solution will be considered regardless of when the installation is completed. Document 2: Client-Issued Supporting Document (Any-One) Even if the installation was completed more than five years ago, Any one of the following client-issued documents: it will still qualify, provided that the same bidder is currently a. Client Credential/Experience Certificate; maintaining that	Please clarify whether the same client/reference can satisfy both the BFSI implementation/maintenance requirement and the cloud implementation requirement, and whether one project can be used for both conditions.	Please refer addendum for revised clause.
789	110-112	10.2 / OEM PQ	SIEM OEM Experience	# Eligibility Criteria/Clause Documents Required 19. The proposed OEM SIEM Solution with a minimum capacity of Document 1: Copy of Purchase Order / Work Order / Contract 30,000 EPS or 1.2 TB/day shall have been successfully The submitted client-issued document shall clearly indicate, either implemented and be under management/maintenance in at least directly or through a combination of documents forming part of the one (1) BFSI in India. same contract: a. Name of the Client. and b. Date of Issue/Signing. c. Scope of Work. The proposed OEM SIEM Solution with a minimum capacity of d. Solution Name and OEM Name 30,000 EPS or 1.2 TB/day shall have been successfully e. SIEM Capacity, clearly indicating one of the following, as implemented on cloud in one (1) in India. applicable: a. Minimum 30,000 EPS or 1.2 TB/day. Note: - OR A bidder's experience in supplying and installing a solution will be considered regardless of when the installation is completed. Document 2: Client-Issued Supporting Document (Any-One) Even if the installation was completed more than five years ago, Any one of the following client-issued documents: it will still qualify, provided that the same bidder is currently a. Client Credential/Experience Certificate; maintaining that	Since RFP requirement is for 50,000 EPS, bidder proposes for strengthening of OEM SIEM PQ to require at least two BFSI deployments in India, at least one at 50,000 EPS/2 TB/day or above, and at least one cloud deployment at comparable scale.	Please refer addendum for revised clause.
790	109	10.2 / Eligibility	Blacklisting	# Eligibility Criteria/Clause Documents Required companies having common director/s or companies in the same group of promoters/management or partnership firms/LLPs having common partners is not owned by any Director or Employee of the Bank. The bidder shall submit a self-declaration confirming that, during the last three (3) years preceding the date of publication of this RFP, no contract, Purchase Order, or award issued by 12. Punjab & Sind Bank (PSB) to the bidder has been cancelled, Self-Certification from the bidder terminated, rescinded, or revoked due to non-performance, breach of obligations, or failure to comply with post-award requirements. The Bidder should not have been blacklisted/ debarred by the Regulator / statutory body/ Government / Government agency 13. Self-Certification from the bidder as per Annexure 11 / Banks / Financial Institutions in India during last 3 years and as on the date of bid submission. The bidder should not be involved in any litigation which 14. Self-Certification from the bidder as per Annexure 10 threatens the solvency of company. 15. Labor Law Compliance Self-Certification from the bidder Document on 100 Rs Stamp paper, duly signed and stamped by the 16. Integrity Pact authorized signatory. Document on 100 Rs Stamp	Please consider extending the lookback to five years and require disclosure of material debarment, contract termination for default, major SLA failure or regulatory enforcement involving the bidder or proposed OEMs.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
791	109	10.2 / Eligibility	Litigation	# Eligibility Criteria/Clause Documents Required companies having common director/s or companies in the same group of promoters/management or partnership firms/LLPs having common partners is not owned by any Director or Employee of the Bank. The bidder shall submit a self-declaration confirming that, during the last three (3) years preceding the date of publication of this RFP, no contract, Purchase Order, or award issued by 12. Punjab & Sind Bank (PSB) to the bidder has been cancelled, Self-Certification from the bidder terminated, rescinded, or revoked due to non-performance, breach of obligations, or failure to comply with post-award requirements. The Bidder should not have been blacklisted/ debarred by the Regulator / statutory body/ Government / Government agency 13. Self-Certification from the bidder as per Annexure 11 / Banks / Financial Institutions in India during last 3 years and as on the date of bid submission. The bidder should not be involved in any litigation which 14. Self-Certification from the bidder as per Annexure 10 threatens the solvency of company. 15. Labor Law Compliance Self-Certification from the bidder Document on 100 Rs Stamp paper, duly signed and stamped by the 16. Integrity Pact authorized signatory. Document on 100 Rs Stamp	Please strengthen this to require disclosure of material cybersecurity, data-protection, IP, fraud, regulatory, service-failure and contract disputes above a defined threshold.	No Change, Please be guided by the RFP
792	108-109	10.2 / Eligibility	Conflict of Interest	# Eligibility Criteria/Clause Documents Required companies having common director/s or companies in the same group of promoters/management or partnership firms/LLPs having common partners is not owned by any Director or Employee of the Bank. The bidder shall submit a self-declaration confirming that, during the last three (3) years preceding the date of publication of this RFP, no contract, Purchase Order, or award issued by 12. Punjab & Sind Bank (PSB) to the bidder has been cancelled, Self-Certification from the bidder terminated, rescinded, or revoked due to non-performance, breach of obligations, or failure to comply with post-award requirements. The Bidder should not have been blacklisted/ debarred by the Regulator / statutory body/ Government / Government agency 13. Self-Certification from the bidder as per Annexure 11 / Banks / Financial Institutions in India during last 3 years and as on the date of bid submission. The bidder should not be involved in any litigation which 14. Self-Certification from the bidder as per Annexure 10 threatens the solvency of company. 15. Labor Law Compliance Self-Certification from the bidder Document on 100 Rs Stamp paper, duly signed and stamped by the 16. Integrity Pact authorized signatory. Document on 100 Rs Stamp	Please require disclosure of all current PSB security contracts held by bidder, OEMs and material affiliates and a conflict assessment covering product/vendor concentration and independent assurance.	No Change, Please be guided by the RFP
793	108-109	10.2 / Eligibility	Conflict of Interest	# Eligibility Criteria/Clause Documents Required companies having common director/s or companies in the same group of promoters/management or partnership firms/LLPs having common partners is not owned by any Director or Employee of the Bank. The bidder shall submit a self-declaration confirming that, during the last three (3) years preceding the date of publication of this RFP, no contract, Purchase Order, or award issued by 12. Punjab & Sind Bank (PSB) to the bidder has been cancelled, Self-Certification from the bidder terminated, rescinded, or revoked due to non-performance, breach of obligations, or failure to comply with post-award requirements. The Bidder should not have been blacklisted/ debarred by the Regulator / statutory body/ Government / Government agency 13. Self-Certification from the bidder as per Annexure 11 / Banks / Financial Institutions in India during last 3 years and as on the date of bid submission. The bidder should not be involved in any litigation which 14. Self-Certification from the bidder as per Annexure 10 threatens the solvency of company. 15. Labor Law Compliance Self-Certification from the bidder Document on 100 Rs Stamp paper, duly signed and stamped by the 16. Integrity Pact authorized signatory. Document on 100 Rs Stamp	Kindly clarify the measures being adopted by the Bank to ensure that there is no conflict of interest with respect to any ongoing or upcoming IT Security RFPs during the period from submission of bids until award of the contract under this RFP.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
794	105-107	10.2 / Eligibility	Multi-Solution Experience	# Eligibility Criteria/Clause Documents Required g. Maintenance / Under Maintenance – Yes/No h. Contract Period: 1. Start Date 2. End Date i. Solution Name. j. OEM Name. k. Implemented SIEM Capacity (EPS and/or TB/day). l. Reference to the submitted client-issued document(s), including: 1. Document Name. 2. Relevant Page Number(s). 3. Clause/Section/Page where the following are evidenced: i. Client Name. ii. Scope of Work. iii. Solution Name. iv. SIEM Capacity (EPS/TB/day). v. Maintenance/Support Status. vi. Contract/Project Period. Bidder should have supplied, installed and maintained (or Bidder to Submit the following 3 Documents: under maintenance) any three (3) of the below solutions in any one PSU/PSE/ Government Organizations / BFSI/Telecom Document 1: Copy of Purchase Order / Work Order / Contract provider in India The submitted client-issued document shall clearly indicate, either 8. a. SOAR directly or through a combination of documents forming part of the b. UEBA same contract: c. Extended Detection & response (XDR)/ Endpoint a. Name of the Client. Detection & response (EDR) b. Date of Issue/Signing.	Please strengthen this to at least five of the listed solutions in one or more BFSI/PSU/Government environments, including at least one of SOAR, UEBA, XDR/EDR, NDR and ITDR.	Please refer addendum for revised clause.
795	105-107	10.2 / Eligibility	Integrated SOC Experience	# Eligibility Criteria/Clause Documents Required d. Network Detection & response (NDR)/Network c. Scope of Work demonstrating supply, installation and Behaviour Anomaly Detection (NBAD) maintenance/AMC/support of the respective Solution. e. Threat Intelligence Platform d. Solution Name and OEM Name f. Vulnerability Assessment/Vulnerability management g. Identity Threat Detection & response AND h. Decoy/Honeypot/Deception i. Application security testing tool (DAST or SAST) Document 2: Client-Issued Supporting Document (Any-One) j. Cloud Security Posture Management (CSPM) Any one of the following client-issued documents: k. Cloud-Native Application Protection Platform (CNAPP) a. Client Credential/Experience Certificate; l. Cloud Workload Protection Platform (CWPP) or m. Continuous Threat Exposure Management (CTEM) b. Email Confirmation from the Client; or Note: - c. Client-signed Installation/Implementation Report; Experience of solutions can be shown in single /multiple or Clients/ work orders meeting the above criteria d. Client Acceptance/Go-Live/Completion/Sign-off Certificate; A bidder's experience in supplying and installing a solution will or be considered regardless of when the installation was e. Extension Letter completed. Even	Please require at least one reference where the bidder integrated SIEM with SOAR plus at least two advanced analytics/response platforms in a production SOC, demonstrating genuine systems-integration capability.	No Change, Please be guided by the RFP
796	103-105	10.2 / Eligibility	SIEM Experience	# Eligibility Criteria/Clause Documents Required Bidder must have at least enrolled manpower (on bidder's Self-certification from the bidder 6. payroll) of 100 experienced employees skilled in areas of Cyber security. The Bidder must have successfully supplied, installed and Bidder to Submit the following 3 Documents: maintained (or under maintenance) SIEM Solution of minimum 20000 EPS / 0.86 TB per day in one PSU/ PSE/ Government Document 1: Copy of Purchase Order / Work Order / Contract Organizations / BFSI/Telecom provider in India in last 5 years The submitted client-issued document shall clearly indicate, either directly or through a combination of documents forming part of the Note: - same contract: A Bidder's experience shall be considered irrespective of when a. Name of the Client. the implementation was completed. Even if the implementation b. Date of Issue/Signing. was completed more than five years prior to the date of c. Scope of Work demonstrating supply, installation and publication of the RFP, such experience shall qualify only where maintenance/AMC/support of the SIEM Solution. the same Bidder that supplied, installed and implemented the d. Solution Name and OEM Name SIEM Solution is also currently maintaining the same solution. e. SIEM	Please increase the minimum bidder SIEM reference to at least 50,000 EPS/2.16 TB/day in production and require the reference to be operational for at least 12 continuous months.	Please refer addendum for revised clause.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
797	103	10.2 / Eligibility	Cyber Manpower	# Eligibility Criteria/Clause Documents Required Bidder must have at least enrolled manpower (on bidder's Self-certification from the bidder 6. payroll) of 100 experienced employees skilled in areas of Cyber security. The Bidder must have successfully supplied, installed and Bidder to Submit the following 3 Documents: maintained (or under maintenance) SIEM Solution of minimum 20000 EPS / 0.86 TB per day in one PSU/ PSE/ Government Document 1: Copy of Purchase Order / Work Order / Contract Organizations / BFSI/Telecom provider in India in last 5 years The submitted client-issued document shall clearly indicate, either directly or through a combination of documents forming part of the Note: - same contract: A Bidder's experience shall be considered irrespective of when a. Name of the Client. the implementation was completed. Even if the implementation b. Date of Issue/Signing. was completed more than five years prior to the date of c. Scope of Work demonstrating supply, installation and publication of the RFP, such experience shall qualify only where maintenance/AMC/support of the SIEM Solution. the same Bidder that supplied, installed and implemented the d. Solution Name and OEM Name SIEM Solution is also currently maintaining the same solution, e. SIEM	Please strengthen this to at least 250 dedicated cybersecurity personnel in India, including a demonstrable SOC/IR/detection-engineering pool, rather than a generic cybersecurity headcount.	Please refer addendum for revised clause.
798	101-128	10.2 / Eligibility	OEM Back-to-Back	# Eligibility Criteria/Clause Documents Required iv. Maintenance/Support Status. v. Contract/Project Period. The proposed OEM services should have been implemented in Document 1: Copy of Purchase Order / Work Order / Contract at least one (1) PSU/ PSE/ Government Organizations / BFSI in The submitted client-issued document shall clearly indicate, either India. directly or through a combination of documents forming part of the same contract: Credential is to be submitted for the following services: a. Name of the Client. 1. Breach Attack & Simulation b. Date of Issue/Signing. 2. Continuous Automated Red Teaming c. Scope of Work demonstrating supply, installation and 3. Attack surface management maintenance/AMC/support of the respective service. 4. Phishing simulation d. Solution Name and OEM Name 5. Anti-phishing services 6. Dark web monitoring OR 7. Brand protection & monitoring 8. Threat Intelligence feed Document 2: Client-Issued Supporting Document (Any-One) 23. 9. Threat Hunting services Any one of the following client-issued documents: a. Client Credential/Experience Certificate; or b. Email Confirmation from the Client; or c. Client-signed Installation/Implementation Report; or d. Client Acceptance/Go-	Please make executed OEM support/back-to-back agreements a pre-award condition for all critical platforms and services, not a post-PO deliverable.	No Change, Please be guided by the RFP
799	101-128	10.2 / Eligibility	Supply Chain Assurance	# Eligibility Criteria/Clause Documents Required 2. SOAR 2. Confirmation that the bidder/entity is duly authorised by the 3. UEBA OEM for supply, installation, implementation, technical support, 4. Extended Detection & response (XDR) maintenance and related services for the proposed solution(s). 5. Network Detection & Response (NDR) The MAF shall be submitted on the official letterhead of the respective 6. Decoy/HoneyPot/Deception OEM and must be signed by an authorised signatory having the 7. Threat Intelligence Platform authority to bind the OEM." 8. Vulnerability Assessment & vulnerability Lifecycle Management 9. Identity Threat Detection & response 10. Application Security Testing 11. Cloud Security Posture Management (CSPM) 12. Cloud-Native Application Protection Platform (CNAPP) 13. Cloud Workload Protection Platform (CWPP) 14. Continuous Threat Exposure Management (CTEM)	Please require critical OEMs to provide software supply-chain assurance including SBOM/CBOM, secure development lifecycle attestation, vulnerability disclosure process and signed commitment to remediate critical product vulnerabilities.	No Change, Please be guided by the RFP
800	101	10.2 / Eligibility	Corporate Experience	Note – In case of MSMEs only, the turnover may be relaxed The CA certificate provided in this regard should be without any riders subject to meeting the quality and technical specifications. or qualification. The bidder should be an authorized representative/ partner/ MAF from the respective OEMs of the solution & services containing- reseller of OEM in India. 1. Name and address of the OEM and the name and address of the 5. authorised bidder/entity. MAF should be submitted from the following solution OEMs: 1. SIEM 10.2 Eligibility Evaluation Criteria # Eligibility Criteria/Clause Documents Required 1. Proof of Earnest Money Deposit To be submitted along with the bid. The Bidder should be operating in India as a registered1. Copy of Certificate of Incorporation or Partnership Deed company under Companies Act, 2013/1956 or LLP (Limited2. AND Liability Partnership) Act 2008 or Partnership firms registered3. Copy of Registration Certificate/GST Registration certificate 2. under the Indian Partnership Act, 1932 with registered offices in India, and should be in existence in India for at least the last Copies of all documents listed above should be attested by authorized 5 (five) years as on date of opening of the bid signatory and must be submitted along with the response. The bidder should have	Please strengthen the criterion to require at least 7 years of relevant cybersecurity/SOC operations experience and at least 3 years of experience delivering managed SOC services to BFSI/PSU/Government clients.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
801	101	10.2 / Eligibility	Turnover	Note – In case of MSMEs only, the turnover may be relaxed The CA certificate provided in this regard should be without any riders subject to meeting the quality and technical specifications. or qualification. The bidder should be an authorized representative/ partner/ MAF from the respective OEMs of the solution & services containing- reseller of OEM in India. 1. Name and address of the OEM and the name and address of the 5. authorised bidder/entity. MAF should be submitted from the following solution OEMs: 1. SIEM 10.2 Eligibility Evaluation Criteria # Eligibility Criteria/Clause Documents Required 1. Proof of Earnest Money Deposit To be submitted along with the bid. The Bidder should be operating in India as a registered1. Copy of Certificate of Incorporation or Partnership Deed company under Companies Act, 2013/1956 or LLP (Limited2. AND Liability Partnership) Act 2008 or Partnership firms registered3. Copy of Registration Certificate/GST Registration certificate 2. under the Indian Partnership Act, 1932 with registered offices in India, and should be in existence in India for at least the last Copies of all documents listed above should be attested by authorized 5 (five) years as on date of opening of the bid signatory and must be submitted along with the response. The bidder should have	Please consider increasing the minimum average India turnover to INR 1,000 crore, with positive net worth and no material adverse qualification in the latest audited financial statements, given the scale and five-year service commitment.	No Change, Please be guided by the RFP
802	100-132	10 EVALUATION CRITERIA	Evaluation Methodology – L1 vs QCBS	# Eligibility Criteria/Clause Documents Required AND	Considering that this is a complex, technology-intensive NextGen SOC transformation involving multiple cybersecurity platforms, OEMs, managed security services, cloud/SaaS architecture, SIEM/UEBA/XDR/NDR/SOAR and advanced services, request the Bank to consider adopting a Quality-and-Cost Based Selection (QCBS) methodology instead of selection solely on L1. A suitable weightage (e.g., 70% Technical/Quality and 30% Commercial) may be considered so that solution capability, architecture, OEM strength, implementation methodology, service delivery model, innovation, security posture and demonstrated experience are appropriately evaluated in addition to price.	No Change, Please be guided by the RFP
803	95 of 1A, 1B	Dark Web Monitoring	Web Logs	Web Logs	Dark Web Monitoring solutions are designed to scan external sources on dark web rather than parse private network traffic or server logs. Could you please confirm	Please refer addendum for revised clause
804	95 of 1A, 1B	Dark Web Monitoring	Payment Intelligence	Payment Intelligence	Could you please provide some more details on it	No Change, Please be guided by the RFP
805	147 of RFP	Service SLAs	Take Down	Site take-down time for identified Phishing URLs – Resolution within 24 hours	We request that the site takedown resolution time for identified phishing URLs be adjusted to a minimum of 48 hours (instead of 24 hours).	No Change, Please be guided by the RFP
806	157of RFP	Penalties	Penalties	For the purpose of this RFP, the total penalties as per LD & SLA will be subject to a maximum of 10% of the overall contract value.	We kindly request that the bank revise the penalty clause to cap penalties per technology at 10% of that specific technology's contract value, rather than the overall contract value	No Change, Please be guided by the RFP RFP Clause 13.2 - For the purpose of this RFP, the total penalties as per LD & SLA will be subject to a maximum of 10% of the overall contract value
807	117	10.2	Eligibility Criteria-Clause-22	The proposed OEM solution should have been implemented in at least one verifiable client in India. Credential is to be submitted for the following solutions: a. CNAPP b. CWPP c. CTEM	CTEM is a new framework and customers are still in evaluation/ Implementation phase. We request you to please consider a change 'Client in India or Global BFSI' The proposed OEM solution should have been implemented in verifiable client in India or Global. Credential is to be submitted for each of the following solutions: 1. CNAPP 2. CWPP 3. CTEM	No Change, Please be guided by the RFP
808	120	10.2	Eligibility Criteria-Clause-23	The proposed OEM services should have been implemented in at least one (1) PSU/ PSE/ Government Organizations / BFSI in India. Credential is to be submitted for the following services: 1. Breach Attack & Simulation 2. Continuous Automated Red Teaming 3. Attack surface management 4. Phishing simulation 5. Anti-phishing services 6. Dark web monitoring 7. Brand protection & monitoring 8. Threat Intelligence feed 9. Threat Hunting services	As the offsite services are specified under the functional compliance requirements and are expected to be provided by the bidder, the corresponding eligibility criteria should be assessed at the bidder level. We request you to please consider a below change 'The proposed bidder services (below mentioned to the services) should have been implemented by the bidder in in at least one verifiable client in India'	No Change, Please be guided by the RFP
809	86	16	Technical Specs-Anti Phishing-	Solution must be able to seamlessly integrate with On-Prem Mail Gateways via Mail Transfer Agent (MTA) forwarding	Anti-Phishing is asked as a Managed service however MTA is a componentfor onprim SEG gateway We request you to please consider a below change 'Solution must be able to seamlessly integrate with On-Prem Mail Gateways via API integration'	Please refer to the relevant Addendum for updated specfications
810	87	18.2	Technical Specs-Anti Phishing-	Solution must provide DoS protection and directory harvest attack protection to ensure the availability of email services	DOS Protection Is Typically the Responsibility of the hardware based Email Infrastructure or Secure Email Gateway or Firewall or dedicated DDOS protection Hence this clause should not fall under Anti-Phishing services We request you to please reconsider this clause	Please refer to the relevant Addendum for updated specfications
811	87	19.2	Technical Specs-Anti Phishing	Solution must be able to display HTML banners on email clients, automatically switching to plain text format if HTML is not supported, while also providing multilingual support based on the organization's language preferences. HTML banner content can be edited or customized by organization	The requirement appears to prescribe a specific notification mechanism (HTML banner insertion) rather than the intended security outcome of user awareness and phishing risk notification. Modern anti-phishing solutions may provide user alerts through native email client warnings, subject tagging, security indicators, API-based notifications, or other mechanisms without relying on HTML banner injection. We request you to please reconsider this clause	Please refer to the relevant Addendum for updated specfications
812	87	19.4	Technical Specs-Anti Phishing	Solution must offer multiple disposition options, including attachment stripping, delivery of notices to senders, and quarantine of the whole email	We request you to please consider a below change 'Solution must offer multiple disposition options, including attachment stripping, and quarantine of the whole email'	Please refer to the relevant Addendum for updated specfications
813	87	19.5	Technical Specs-Anti Phishing	Solution must provide a "Safe Preview" capability for administrators to view detailed information of quarantined messages and decide necessary actions	We request you to please consider a below change Solution must provide a "Safe Preview of links" capability for administrators to view detailed information of quarantined messages and decide necessary actions	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
814	88	19.8	Technical Specs-Anti Phishing-	As part of the forensic collection, should include the capture of PowerShell history	The requirement appears to mandate a specific forensic artefact (PowerShell history) rather than the intended security objective of investigating PowerShell-based activity. We request you to please consider a below change As part of the forensic collection, should include the capture of PowerShell history or equivalent forensic mechanism	Please refer to the relevant Addendum for updated specfications
815	88	19.17	Technical Specs-Anti Phishing-	Solution must provide detailed reporting covering system usage and other areas including global message summary, spam, virus and other rule actions to save administrator time and effort in the collection of data for status reports. Reports can be emailed (HTML), printed, or downloaded in CSV format for use with third party tools	We request you to please consider a below change Solution must provide detailed reporting covering system usage and other areas including global message summary, spam, virus and other rule actions to save administrator time and effort in the collection of data for status reports. Reports can be emailed (HTML), printed, or downloaded in CSV or PDF format for use with third party tools	Please refer to the relevant Addendum for updated specfications
816	88	19.18	Technical Specs-Anti Phishing-	Solution must have capability for administrators to view reports containing detailed statistics covering emails processed, rejected emails, SMTP transactions, and communication flows	The requirement mandates visibility into SMTP transactions and communication flow analytics, which are traditionally functions of MTA,and may not have direct access in API-based or cloud-native anti-phishing solutions. We request you to please consider a below change Solution must have capability for administrators to view reports containing detailed statistics covering emails processed, rejected emails.	Please refer to the relevant Addendum for updated specfications
817	89	19.37	Technical Specs-Anti Phishing-	Solution must support message classification management, including separate classifiers for spam, impersonation, bulk, phishing, adult, and malware messages, with the ability to set score thresholds per category.	The requirement mandates a specific detection architecture based on separate classifiers and per-category scoring thresholds. Modern email security and anti-phishing solutions increasingly leverage AI/ML models, behavioural analytics, graph intelligence, and composite risk engines that may not expose individual classifiers We request you to please consider a below change Solution must support message classification management, including separate classifiers for spam, impersonation, bulk, phishing and malware messages, with the ability to set score thresholds per category.	Please refer to the relevant Addendum for updated specfications
818	89	19.41	Technical Specs-Anti Phishing	Solution must provide granular administrative controls to allow role-based access to each module and quarantine folder.	Modern cloud-native anti-phishing solutions implement administrative segregation through configurable RBAC, delegated administration, role groups, and permission-based access models, which may not necessarily expose permissions at the individual module or quarantine-folder level We request you to please consider a below change Solution must provide granular administrative controls to allow role-based access	Please refer to the relevant Addendum for updated specfications
819	89	19.43	Technical Specs-Anti Phishing	Solution must support complicated mail routing requirements, including group-based routing based on user groups	The requirement appears to address email infrastructure and mail-flow routing capabilities rather than core anti-phishing or email threat protection functionality. Complex mail routing, transport rules, and group-based routing are typically implemented within the email platform We request you to please reconsider this clause	Please refer to the relevant Addendum for updated specfications
820	89	19.5 0	Technical Specs-Anti Phishing	solution must support a range of routing behaviors and actions for different scenarios, allowing administrators to customize email handling based on specific needs and requirements.	The requirement is broad and appears to focus on email routing and mail-flow management capabilities, which are typically functions of the email infrastructure (Microsoft Exchange, Exchange Online We request you to please reconsider this clause	Please refer to the relevant Addendum for updated specfications
821	90	19.51	Technical Specs-Anti Phishing	Solution must support for in outbound or inbound email including footer management Inserting one or more legal or compliance footers (e.g. disclaimer) Multi-language support Apply different filters based on email attributes or active directory attributes, Insert dynamic content to footer such as date, when to apply the footer in the message routing hops, Selectively apply based on policy / attribute or not apply if the email is s/mime encrypted or digitally signed, etc Apply signatures and disclaimers based on AD user groups	Footer management is vendor specific feature We request you to please reconsider this clause	Please refer to the relevant Addendum for updated specfications
822	90	19.5 3	Technical Specs-Anti Phishing	Solution must allow end-users to receive customized email notifications based on domain name.	The clause prescribes a specific notification customization method (domain-based) that may not be supported by all modern cloud-native Anti-Phishing solution We request you to please consider a below change Solution must allow end-users to receive customized email notifications based alerts, and awareness messages based on organizational policies	Please refer to the relevant Addendum for updated specfications
823	90	19.5 7	Technical Specs-Anti Phishing	Solution must provide administrators with capabilities for email queue management	This feature is exchange or onprem gateway specific. We request you to please reconsider this clause	Please refer to the relevant Addendum for updated specfications
824	90	19.5 9	Technical Specs-Anti Phishing	Solution must support alerting the security team on all policies, quarantine folders, and queue thresholds	The clause is a gateway-specific alerting model based on quarantine folders and queue thresholds. Modern cloud-native email security solutions may not utilise traditional mail queues while still providing comprehensive alerting for security incidents, policy actions, quarantine events, and operational status We request you to please consider a below change Solution must support alerting the security team on all policies, quarantine folders, and queue thresholds or equivalent alerting mechanism	Please refer to the relevant Addendum for updated specfications
825	90	19.6 2	Technical Specs-Anti Phishing	Solution must provide application and message routing troubleshooting tools with a message-tracing capability to facilitate help desk work	Message routing trobleshooting & message-tracing capabilities are part of exchange provider. We request you to please reconsider this clause	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
826	30	7.2.1 Solutions – Master Deployment Matrix	#8. Vulnerability assessment (VA) & vulnerability lifecycle management	Bank Location: Standalone at DC and Standalone at DR. Management Console: Deployed at both DC and DR	As per this RFP Technical Specification of VA & VLM,document #1788963129, #12 "The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and failover capabilities" where the 7.2.1 of suggests standalone deployment at DC, DR and console availablity at both DC and DR. These two partially contradict each other. We request you to kindly confirm if standalone VA & VM in DC and DR are expected to function independently. Maintaining two standalone environments with both consoles accessibility will lead to duplication of vulnerabilities, configuration efforts and it will cost upto 2X in terms of licensing. Though its not clear but we assume that you need one VM in DC and one in DR where primary one shares configuration backup on secondary and secondary can take over when the primary goes down, the primary VM solution should be able to scan both the DCs and vice-versa. If this understanding is correct, kindly update the clause as following - 'The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and active-cold standby failover capabilities where only one active console shall be accessible at a time'.	No Change, Please be guided by the RFP
827	260	16.21.2 Volumetrics-Solution-wise Requirements	10 Vulnerability Assessment & Management (VA-VM) Minimum Numbers of IPs: 4000	10 Vulnerability Assessment & Management (VA-VM) Minimum Numbers of IPs: 4000	As per the RFP #1788963158, page 257 16.21.1 Current IT assets, P&SB has 2500 servers, 300 DB, 200 Apps, 12000 endpoints/desktops and 7200 routers and switches whereas the VA/VM IP coverage is mention as "Minimum" 4000. We seek your guidance and confirmation on the final count of assets/IPs you need coverage from day #1, given "minimum" count may lead to each bidder proposing seperate numbers and very likely excluding important assets from highly important VA & VM exercise. Without a defined and finite asset count, bidders cannot be compared on a like-for-like basis as the ones concerned about the VA/VM security posture of the infra will propose to cover more IPs/Assets while some may cover bare minimum and appear more competitive. We request you to kindly provide the final IP count required for VA/VM from day #1 considering the licenses are bound to assets and deleting the asset will delete all historic vulnerability and trends data, deleted asset will not cover alerts, ITSM integration and cannot be considered as part of VM exercise. As per the CERT'in recommendations (https://www.cert-in.org.in/PDF/guidelinesgovtentities.pdf) as well as industry best practices, entire ICT infrastructure should be part of the vulnerability management exercise and network device inclusion is absolute must given these are critical assets and in some zones exposed directly to internet.	No Change, Please be guided by the RFP
828	38	On premises deployment of solutions	Storage Capacity & Sizing	• The Bidder shall provide detailed storage sizing based on expected data/log volumes, peak ingestion rate, retention period, indexing, enrichment, compression, replication, backup, archival and anticipated annual growth. Adequate capacity shall be provisioned for the complete contract period.	As per the RFP #1788963158, storage duration on the primary storage of the solution itself is mention for Cloud/SaaS/Hybrid to be 3 months, same is not clearly specified for VA & VM. Kindly confirm how long should the VA & VM solution retain the asset, vulnerability, logs, activities, historic trend etc. As per CERT-IN it must be 6 months. Kindly confirm if you wish the solution to retain this info on its own primary storage to be for 6 months or less.	Please refer addendum for revised clause
829	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - VA-VM	VA-VM S.No. 9	Each scanning engine shall support web application security assessment together with traditional infrastructure vulnerability and configuration/compliance assessment. The solution shall identify vulnerabilities, missing patches, insecure configurations, and compliance deviations, and generate comprehensive reports containing risk severity, evidence of findings, affected assets, and remediation recommendations to support security governance, audit, and regulatory compliance.	While its possible to perform this via VA VM solution with additional WAS/DAST license, this will be a duplication of solution given you are already asking for seperate 'Application Security Testing Tool'. Hence, we request you to kindly move the 'Web application security assessment' from VA & VM requirements to DAST as this is a DAST requirement and may unnecessorily require to duplicate the licenses, solution and hardware.	No Change, Please be guided by the RFP
830	Functional Compliance Sheet pp.48-51 (Appendix 1A)	Appendix 1A - VA-VM	VA-VM S.No. 36-52 and S.No. 61-77; S.No. 87 and S.No. 89	All technical compliances of VA-VM S.No. 36-52 and S.No. 61-77; S.No. 87 and S.No. 89	S.N 61-77 are likely duplicates of S.N 36 to 52 with minor changes. Request you to kindly review and confirm if this is intentional or typo. If not intentional, we request you to please reconsider duplicates to have the score calculated accordingly.	No Change, Please be guided by the RFP
831	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 12	The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and failover capabilities.	VM solution is not an inline and always active solution.VM solutions across the industry do not have failovers similar to inline solutions such as firewalls. Hence, we request you to kindly consider the failover scenario as active - cold standby with documented backup-restore and a controlled switchover in place of automatic console failover. We request you to please consider a below change The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and failover capabilities either automatically or using manual and controlled backup restore.	No Change, Please be guided by the RFP
832	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 15	The proposed solution shall support integration with SIEM, SOAR, Threat Intelligence Platforms, NAC, and other security platforms through APIs or standard integration mechanisms.	Kindly share details (Vendor/Model/Version) of the SIEM, SOAR, TIP and NAC solution you would want to integrate with for us to identify the availablity of standard or API based integration and accordingly finalize the deployment efforts.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
833	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 16	The proposed solution shall integrate with Privileged Access Management (PAM) solutions for secure credential management during authenticated scans.	Kindly share details (Vendor/Model/Version) of the PAM solution you would want to integrate with for us to identify the availablity of integration and also identify the deployment efforts.	Bank is currently procuring PAM solution through separate RFP.
834	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 17	The proposed solution shall integrate with IT Service Management (ITSM) and ticketing platforms for automated vulnerability tracking and remediation workflows.	Could you please share details (Vendor/Model/Version) of the ITSM solution you would want to integrate with for us to identify the availablity of standard or API based integration and accordingly finalize the deployment efforts.	ITSM - Manage Engine
835	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 29	The proposed solution shall support vulnerability assessment and compliance reporting aligned with PCI DSS requirements.	We request you to kindly confirm whether you only require to perform PCI DSS internal scanning and reporting on-premises or you also require the PCI- ASV attestation. If Attestation is required, could you please share the exact asset count for which the attestation is needed and how many attestations are to be submitted within 1 year.	No Change, Please be guided by the RFP
836	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 42	The solution shall support vulnerability assessment of VMware ESXi, Hyper-V, Nutanix AHV, Kubernetes, OpenShift and container platforms.	We request you to kindly confirm whether you need the OS and platform vulnerability assessment of these container solutions or you need a comprehensive container security solution with the ability to identity vulnerabilities of images, registries and their components. If you need comprehensive container security assessment, we request you to kinly move this required to CNAPP solution as its usually part of cloud security solutions and not VM solution.	No Change, Please be guided by the RFP
837	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 47	The solution shall support Multi-Factor Authentication (MFA), LDAP, Active Directory, SAML 2.0 and OpenID Connect authentication.	We request you to kindly reconsider the OpenID and request you to please consider a below change - The solution shall support Multi-Factor Authentication (MFA via SAML and/or LDAP), LDAP, Active Directory, SAML 2.0.	No Change, Please be guided by the RFP
838	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 48	The solution shall support secure encrypted communication using TLS 1.3 and cryptographic modules compliant with FIPS 140-3 or equivalent internationally recognized standards.	We request you to kindly allow the FIPS 140-2 or equivilent solution transitioning to FIPS 140-3 to participate and request you to please consider a below change The solution shall support secure encrypted communication using TLS 1.3 and cryptographic modules compliant with FIPS 140-2 or FIPS 140-3 or equivalent internationally recognized standards.	Please refer addendum for revised clause
839	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 51	The solution shall identify internet-facing assets and continuously monitor externally exposed services.	We request you to kindly reconsider this clause as its an ASM(Attack Surface Management) requirements which is already asked separate service based solution of the RFP.	Please refer the addendum for revised clause
840	Functional Compliance Sheet p.49 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 56	The solution shall support digitally signed and password-protected reports with configurable retention and archival.	We request you to please consider a below change The solution shall support password-protected reports with configurable retention and archival.	Please refer addendum for revised clause
841	Functional Compliance Sheet p.49 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 60	The solution shall provide comprehensive REST APIs and webhook support for automation and integration with enterprise security platforms.	We request you to please consider a below change The solution shall provide comprehensive REST APIs or webhook support for automation and integration with enterprise security platforms.	Please refer addendum for revised clause
842	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 87	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	We request you to kindly reconsider this clause from VM and move it to CTEM as this is a CTEM requirement, a solution that can be cloud/SaaS based. Given the data soveraginity and sensitivity of bank's vulnerabilities data, the platform is correctly requested to be on-prem which shall also be able to function without any internet connectivity. Hence, AI powering the on-prem application to achieve all the listed items is not viable.	Please refer addendum for revised clause
843	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 88	Unified, correlated findings intelligence. Every scanning engine — across web, API, network and host, cloud, containers, mobile, source code, device configuration and identity — reports into a single normalized findings model..	This is a CTEM requirement as VM solution won't perform VA of source code, identity etc. We request you to kindly reconsider this clause from VM and move it to CTEM	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
844	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 89	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	This is a duplicate of S.N. #87, we request you to please reconsider this clause	Please refer addendum for revised clause
845	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 90	Mobile Application Security Testing: The proposed solution shall support static security analysis of Android and iOS mobile application packages, including APK/AAB and IPA formats, and shall provide security assessment mapped to recognized mobile application security standards and methodologies such as OWASP MASVS and MASTG.	This is not part of any VA/VM solution in industry and belongs to application security testing. We request you to kindly move this to 'Application Security Testing Tool'.	No Change, Please be guided by the RFP
846	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 91	White-Label Reporting and Approval Workflow: The proposed solution shall support customizable/white-label security assessment reports, including organization-specific branding and configurable report content. The solution shall support role-based maker-checker workflow for report generation, review, approval, and controlled release of finalized reports.	We request you to please consider a below change White-Label Reporting and Approval Workflow: The proposed solution shall support customizable/white-label security assessment reports, including organization-specific branding and configurable report content. The solution shall support role-based access for report generation, review of the finalized reports.	Please refer addendum for revised clause
847	92	7.18.1 Compute Infrastructure	10. Non-production:	10. Non-production: a) The non-production environments should have the same software and hardware setup as deployed in production environments meeting all RFP requirements.	While this clause suggests the hardware and software setup of non-prod to be same, "16.21 Annexure 21: Sizing/Volumetrics, Data Retention and Current Infrastructure" suggests the VM based solution to have minimum 10% size. Kindly confirm if the 10% requirement of non-production infra is for only licenses whereas the hardware specs are to be identical to prod or both the licenses as well as hardware/software specs to be 10% of the production infra. Also kindly confirm if the non-production is to be setup only at DC or DC as well as DR.	Please refer addendum for the revised clause
848	Functional Compliance Sheet pp.47-51 (Appendix 1A)	Appendix 1A - VA-VM	TOTAL MARKS row and S.No. 1 to 94	TOTAL MARKS - 850	While the VA-VM section contains 94 scoreable clauses, each carrying Maximum Marks of 10, which totals 940 marks, whereas the TOTAL MARKS row of the section states 850. We request you to kindly publish the corrected total and confirm the marks allocated per clause, so that bidders can compute the Respective Solution Compliance required by the Appendix 1A summary sheet consistently.	Please refer addendum for the revised clause
849	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 19, 20, 43 and 44 (missing) and TOTAL MARKS row	CNAPP section is numbered from S.No. 1 to S.No. 60; however S.No. 19, 20, 43 and 44 do not appear in the sheet. TOTAL MARKS - 560.	The CNAPP section is numbered up to S.No. 60 but S.No. 19, 20, 43 and 44 are not present, leaving 56 scoreable clauses which, at 10 marks each, reconciles to the stated TOTAL MARKS of 560. We request you to kindly confirm whether these four clauses have been intentionally deleted or have been inadvertently omitted from the published sheet. If clauses exist against these serial numbers, kindly publish them along with the revised TOTAL MARKS; if they have been deleted, kindly re-issue the sheet with continuous numbering so that bidders' compliance responses and score computation remain traceable to the Bank's evaluation sheet.	Please refer addendum for the revised clause
850	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 16	The solution shall support integration with relevant source-code repositories, development tools, build systems, CI/CD platforms and security workflows, either natively or through supported connectors/APIs.	A CNAPP integrates with source-code repositories and CI/CD platforms for Infrastructure-as-Code (IaC), container image and cloud-configuration assessment. It does not act as a source-code security testing tool, which is the function of the separately procured 'Application Security Testing Tool' in this RFP. We request you to please consider a below change: "The solution shall support integration with relevant source-code repositories, development tools, build systems, CI/CD platforms and security workflows, either natively or through supported connectors/APIs, for the purpose of Infrastructure-as-Code, container image and cloud configuration assessment."	No Change, Please be guided by the RFP
851	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 17 and S.No. 18	S.No. 17 - The solution shall identify security risks and known vulnerabilities associated with third-party, open-source and externally sourced software components and dependencies used by cloud-native applications. S.No. 18 - The solution shall provide visibility into application dependencies and software components and shall identify affected applications where a vulnerable component or dependency is detected.	Identification of third-party/open-source components and application dependencies is a Software Composition Analysis (SCA)/SBOM capability which belongs to the 'Application Security Testing Tool' scope already sought separately in this RFP, and requiring it again under CNAPP will lead to duplication of licences and cost without additional security benefit to the Bank. We request you to kindly either move these clauses to the Application Security Testing Tool requirements, or update them as following - "The solution shall identify known vulnerabilities in third-party and open-source software components and dependencies present within container images, registries and cloud workloads assessed by the platform, and shall identify the affected cloud-native applications/components."	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
852	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 24	The solution shall provide security visibility for cloud-native APIs and application interfaces, including risks related to exposure, authentication, authorization, access control and relevant configurations, where supported.	Discovery and security assessment of application APIs (including authentication/authorization testing of API endpoints) is the function of a dedicated API Security/API posture solution, and is not a native capability of CNAPP platforms. CNAPP platforms provide visibility of cloud-native API gateway and managed API service configurations and their exposure. We request you to please consider a below change: "The solution shall provide security visibility for cloud-provider API gateway/managed API services and application interfaces discovered from the cloud control plane, including risks related to public exposure, authentication/authorization configuration and access control settings, where supported by the respective cloud platform."	No Change, Please be guided by the RFP
853	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 26	The solution shall provide visibility into application access to sensitive or critical data and identify security risks arising from inappropriate application access, exposure or relationships, where supported.	As worded, this clause can be read as requiring full Data Security Posture Management (DSPM) with data discovery and classification of the Bank's data stores, which is a separately licensable product category and is not part of a baseline CNAPP. We request you to kindly confirm whether DSPM (data discovery and classification) is intended to be in scope of the CNAPP. If it is not intended, We request you to kindly ammend the clause as following - "The solution shall provide visibility into application and identity access paths to cloud data stores and shall identify security risks arising from public exposure, excessive access or inappropriate relationships to such data stores, where supported by the respective cloud platform." If DSPM is intended, kindly publish the applicable volumetrics (number/size of data stores) so that bidders can size and price the module consistently.	No Change, Please be guided by the RFP
854	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 27	The solution shall identify vulnerable application components that are reachable, exposed or potentially exploitable within the application's dependency or relationship graph, where such analysis is supported.	Code-level 'reachability' analysis of a vulnerable function within an application's dependency graph is an SCA/ASPM capability delivered by application security testing tools. CNAPP platforms determine exposure and exploitability from cloud context - internet exposure, network path, identity privilege and attack-path relationships. We request you to please consider a below change: "The solution shall identify vulnerable application components that are internet-exposed, network-reachable or potentially exploitable based on cloud exposure, network path, identity privilege and attack-path relationship analysis, where such analysis is supported by the proposed solution."	No Change, Please be guided by the RFP
855	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 32	The solution shall provide guided, semi-automated and/or automated remediation capabilities for supported application-security findings.	Fully automated remediation executed directly by a security platform on a production banking cloud environment is generally not permitted under change-management controls, and CNAPP platforms deliver remediation as guided steps and auto-generated remediation artefacts (e.g., IaC fix code/pull requests, CLI commands, policy snippets) which are then applied by the Bank/implementation partner through the Bank's change process. We request you to please consider a below change: "The solution shall provide guided remediation and automatically generated remediation artefacts (such as IaC remediation code, pull requests, CLI commands or policy snippets) for supported application-security findings, which may be applied through the Bank's approved change-management process or through integration with the Bank's SOAR/ITSM platform."	No Change, Please be guided by the RFP
856	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 59	The solution shall support high availability and service continuity appropriate to the proposed deployment architecture and shall provide mechanisms for recovery of relevant configurations, policies and security information.	Where the CNAPP is delivered as OEM-managed SaaS, high availability, redundancy, backup and disaster recovery are provided by the OEM within the platform and are governed by the OEM's published availability SLA; the Bank cannot be provided Bank-operated HA/DR or restore mechanisms for a SaaS platform. We request you to please consider a below change: "For SaaS-delivered solutions, the OEM shall provide high availability, redundancy and disaster recovery within the platform in line with its published availability SLA, and shall provide mechanisms for export/retrieval of relevant configurations, policies and security information. For on-premises components, if any, the solution shall support HA and documented backup-restore."	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
857	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP - Section scope (S.No. 1 to 50, principally S.No. 1, 6, 7, 8 to 41)	The proposed Cloud Workload Protection Platform (CWPP) shall provide centralized capabilities for protecting, monitoring, detecting, investigating and responding to security threats affecting cloud workloads during runtime. (S.No. 1) and the runtime detection, prevention, response, forensics and threat-hunting clauses at S.No. 6 to 41.	The CWPP section as drafted is predominantly a runtime endpoint/server threat prevention, detection and response (EDR/XDR-class) specification - in-guest malware and ransomware prevention, exploit prevention, host IDS/IPS, file integrity monitoring, process and command-line telemetry, containment actions such as process termination, file quarantine and workload isolation, forensic timelines, process trees and threat hunting. These are delivered by an EDR/XDR agent platform, whereas the CNAPP/CWPP category referenced elsewhere in this RFP delivers agentless workload vulnerability, malware, misconfiguration, identity, secrets and exposure assessment with attack-path context. Given the Bank is separately procuring EDR/XDR and SOC/SIEM capabilities under this very RFP, we request you to kindly clarify and confirm any one of the following, so that bidders are not compelled to bid a second endpoint agent on the same servers: 1. That runtime prevention, containment and forensics requirements of the CWPP section may be met through the Bank's in-scope EDR/XDR platform, with the CWPP providing agentless workload exposure assessment, posture and attack-path context integrated with it; or 2. That the CWPP section may be responded to on a multi-OEM/consortium basis with clear identification of the product meeting each clause (consistent with S.No. 50 of this section); or 3. That the runtime prevention/response clauses be moved	No Change, Please be guided by the RFP
858	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 2 and S.No. 3	S.No. 2 - The solution shall support protection of workloads deployed across physical, virtual, private-cloud, public-cloud and hybrid-cloud environments, as applicable. S.No. 3 - The solution shall support major public-cloud environments including AWS, Microsoft Azure and Google Cloud Platform, as applicable.	CWPP licensing and sizing depend entirely on the workload inventory in scope, and the clause extends coverage to physical and private-cloud workloads in addition to public cloud. We request you to kindly publish, for the CWPP scope, the workload volumetrics for day #1 and for the contract period - number of physical servers, virtual machines, public-cloud instances (per CSP), container hosts/nodes, Kubernetes clusters and serverless functions - along with the CSP accounts/subscriptions/projects in scope. Kindly also confirm which of these environments are mandatory on day #1, since 'as applicable' may lead each bidder to price a different scope and render the commercial bids non-comparable.	No Change, Please be guided by the RFP
859	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 8, S.No. 21 and S.No. 22	S.No. 8 - The solution shall detect and prevent, where supported, malware, ransomware, trojans, rootkits and other malicious software or activities affecting protected workloads. S.No. 21 - The solution shall provide protection against ransomware and destructive activities, including detection of abnormal file encryption or mass file modification behavior. S.No. 22 - The solution shall provide exploit detection and/or prevention capabilities for supported workload operating systems and applications.	In-guest prevention of malware, ransomware, trojans and rootkits, behavioural detection of mass file-encryption, and memory/exploit prevention require a kernel-level endpoint prevention engine (EDR/EPP) and are not functions of an agentless cloud workload protection platform, which performs malware and vulnerability detection through workload snapshot/disk analysis without in-line blocking. We request you to kindly move these clauses to the EDR/XDR section of the RFP, or update them as following - "The solution shall detect malware, ransomware, trojans, rootkits, malicious files and destructive activity affecting protected workloads through agentless and/or agent-based assessment, and shall support prevention/blocking natively or through integration with the Bank's EDR/XDR platform."	S.No. 8- No Change, Please be guided by the RFP S.No. 21- No Change, Please be guided by the RFP S.No. 22- No Change, Please be guided by the RFP
860	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 9 to S.No. 14	S.No. 9 to 14 - monitoring of process execution and process behaviour; detection of suspicious process chains and abnormal parent-child relationships; monitoring of command-line execution, scripts and interpreters; detection of Living-off-the-Land techniques; behavioural/heuristic analysis of anomalous activity; and detection of privilege escalation, persistence, lateral movement and credential misuse.	These clauses describe in-guest runtime behavioural telemetry (process, command-line, script and parent-child process monitoring) which is collected by an EDR/XDR sensor and analysed in the SOC/SIEM. A CWPP that assesses workload exposure agentlessly does not generate kernel-level process telemetry. We request you to kindly move these clauses to the EDR/XDR section, or update them as following - "The solution shall provide the specified runtime behavioural detection capabilities natively or through correlation of telemetry from the Bank's EDR/XDR and SIEM platforms, and shall enrich such detections with workload vulnerability, identity, configuration and exposure context." Kindly also confirm that a capability delivered through such integration will not be treated as non-compliant, consistent with the principle already accepted at CNAPP S.No. 53 of this Appendix.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
861	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 15, S.No. 16 and S.No. 17	S.No. 15 - The solution shall monitor relevant network communications involving protected workloads and identify suspicious or unauthorized communication patterns. S.No. 16 - The solution shall identify communication with known or suspected malicious infrastructure, including malicious IP addresses, domains, URLs, command-and-control infrastructure or equivalent threat indicators, where applicable. S.No. 17 - The solution shall provide host/workload-based intrusion detection and/or prevention capabilities for supported operating systems and workloads.	Host-based intrusion detection/prevention and in-line inspection of workload network traffic for command-and-control communication are functions of HIDS/HIPS agents, NDR and NGFW/IPS controls, all of which are separately in scope in this RFP. A CWPP provides network exposure and reachability analysis from cloud configuration (security groups, NACLs, routes, load balancers, public exposure) rather than packet-level inspection. We request you to kindly move these clauses to the EDR/XDR, NDR or NGFW sections as appropriate, or update them as following - "The solution shall identify workload network exposure, reachable paths and unauthorized/high-risk communication paths from cloud network configuration and available flow logs, and shall support identification of communication with known malicious infrastructure natively or through integration with the Bank's EDR/XDR, NDR, NGFW and SIEM platforms."	S.No. 15- No Change, Please be guided by the RFP S.No. 16- No Change, Please be guided by the RFP S.No. 17- No Change, Please be guided by the RFP
862	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 18 and S.No. 19	S.No. 18 - The solution shall monitor critical files, directories, system objects and configuration elements for unauthorized modification, creation or deletion, where supported. S.No. 19 - The solution shall provide file integrity monitoring for designated critical files, directories and system objects.	File Integrity Monitoring (FIM) requires a resident agent performing real-time file-system event monitoring on the workload and is a standard EDR/host-integrity capability. It is not delivered by an agentless cloud workload protection platform. We request you to kindly move these clauses to the EDR/XDR section, or update them as following - "File integrity monitoring for designated critical files, directories and system objects shall be provided natively or through integration with the Bank's EDR/XDR or host-integrity solution, with the resulting events available for correlation and reporting."	No Change, Please be guided by the RFP
863	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 20 and S.No. 24	S.No. 20 - The solution shall detect suspicious creation or modification of system accounts, services, scheduled tasks and other persistence mechanisms, where applicable. S.No. 24 - The solution shall support detection and/or prevention of web-shell and other unauthorized application-level persistence mechanisms, where applicable.	Real-time detection of persistence mechanisms and prevention of web-shell execution are runtime endpoint and web application protection (EDR/WAF) functions. A CWPP can identify such artefacts through periodic workload assessment but cannot prevent their execution. We request you to kindly move these clauses to the EDR/XDR and WAF sections respectively, or update them as following - "The solution shall identify unauthorized accounts, services, scheduled tasks, web-shells and other persistence artefacts present on assessed workloads, and shall support real-time detection/prevention natively or through integration with the Bank's EDR/XDR and WAF platforms."	No Change, Please be guided by the RFP
864	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 23	The solution shall support virtual patching or equivalent compensating protection mechanisms, where applicable, for vulnerabilities for which immediate patching is not feasible.	Virtual patching is enforced by in-line controls - host IPS agents, NGFW/IPS and WAF - all of which are separately procured under this RFP. A workload protection/exposure platform identifies the vulnerability and recommends the compensating control; it does not itself enforce a virtual patch. We request you to kindly reconsider this clause from the CWPP section as it is already covered by the Bank's NGFW/IPS and WAF requirements, or update it as following - "For vulnerabilities where immediate patching is not feasible, the solution shall identify the exposure, provide risk context and recommend applicable compensating controls, which may be enforced through the Bank's in-line security controls (host IPS, NGFW/IPS, WAF) through supported integration."	No Change, Please be guided by the RFP
865	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 25, 26, 27 and 28	S.No. 25 - runtime security monitoring and threat detection for containerized workloads; S.No. 26 - runtime protection for Kubernetes workloads including pods, containers and workload processes; S.No. 27 - detection of suspicious behaviour involving containers, pods, workload processes and workload-to-workload communications; S.No. 28 - security monitoring for serverless workloads/functions.	Container and Kubernetes runtime protection requires a privileged runtime sensor (e.g., eBPF/DaemonSet-based) on every node, which materially differs from the container and Kubernetes security posture, image/registry scanning, admission control and Kubernetes misconfiguration and RBAC assessment delivered by a CNAPP/CWPP. We request you to kindly clarify whether the Bank requires (a) container/Kubernetes runtime sensor-based prevention or (b) container and Kubernetes security posture with image, registry, IaC, admission-control and RBAC assessment plus runtime detection through the Bank's EDR/XDR on the worker nodes. We request you to kindly permit option (b) and update the clauses to allow the capability to be delivered through posture assessment, admission control and integration with the Bank's EDR/XDR and SIEM, failing which the clause is restrictive to a small subset of OEMs. Kindly also publish the number of Kubernetes clusters, nodes and serverless functions in scope for sizing.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
866	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 29 and S.No. 30	S.No. 29 - The solution shall support agent-based and/or agentless protection mechanisms, as applicable to different workload types and supported environments. S.No. 30 - Where an agent is required, the solution shall provide mechanisms for secure deployment, centralized management, health monitoring and controlled upgrade of the workload protection agent.	We note and appreciate that S.No. 29 permits agentless mechanisms. However, several other clauses in this section (S.No. 8 to 41) are achievable only through an in-guest agent, which contradicts the option provided in S.No. 29. We request you to kindly confirm that an agentless-first architecture, supplemented where required by the Bank's EDR/XDR agent already deployed on the workloads, will be accepted as compliant against this section, and that S.No. 30 shall apply only where the bidder proposes its own agent. Kindly also confirm that no additional agent is mandated on workloads that already carry the Bank's EDR/XDR agent, in view of performance and change-management impact on production banking workloads.	No Change, Please be guided by the RFP
867	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 32 and S.No. 33	S.No. 32 - The solution shall support configurable response actions for detected threats, including alerting, blocking, process termination, file quarantine, workload isolation or other equivalent containment actions, as applicable. S.No. 33 - The solution shall provide workload isolation or containment capabilities to limit the impact or spread of a confirmed or suspected compromise, where supported.	Process termination, file quarantine and host/network isolation are kernel-level containment actions performed by an EDR/XDR agent. An agentless workload protection platform performs cloud-control-plane actions (such as snapshotting, tagging, security-group/identity restriction) and orchestrates containment through the Bank's EDR/XDR and SOAR. We request you to kindly move these clauses to the EDR/XDR section, or update them as following - "The solution shall support configurable response actions for detected threats, including alerting, notification, cloud-control-plane containment actions (such as network/identity restriction, snapshot and tagging) natively, and process termination, file quarantine and workload isolation through integration with the Bank's EDR/XDR and SOAR platforms."	S.No. 32 - No Change, Please be guided by the RFP S.No. 33 - No Change, Please be guided by the RFP
868	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 34, 35, 36 and 37	S.No. 34 - security investigation using process, file, network, user, workload and event-level information; S.No. 35 - historical workload activity and security-event information sufficient for investigation and forensic analysis; S.No. 36 - process-tree or equivalent process-relationship visualization; S.No. 37 - workload-level threat hunting using available security telemetry and configurable search criteria.	Retention of process/file/network event-level telemetry, process-tree reconstruction and telemetry-based threat hunting are EDR/XDR and SIEM functions and require an in-guest sensor. Additionally, these clauses do not specify a retention period, which makes consistent sizing and pricing impossible. We request you to kindly (a) move these clauses to the EDR/XDR and SIEM sections or permit compliance through integration with the Bank's EDR/XDR and SIEM platforms, and (b) if retained under CWPP, publish the mandated telemetry retention period (hot/warm/archive) and the expected daily event volume per workload, so that all bidders size storage and licences on a common basis.	No Change, Please be guided by the RFP
869	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 38 and S.No. 39	S.No. 38 - The solution shall support identification and searching of Indicators of Compromise (IoCs), including supported hashes, IP addresses, domains, URLs and equivalent indicators. S.No. 39 - The solution shall support integration with external threat-intelligence sources to enhance workload threat detection and investigation.	Retrospective and real-time IoC sweeps across workloads are performed on EDR/XDR telemetry or in the SIEM, where the Bank's threat-intelligence platform feeds are already consolidated under this RFP. We request you to please consider a below change: "The solution shall support identification and searching of Indicators of Compromise (hashes, IP addresses, domains, URLs and equivalent indicators) against available workload assessment data natively, and across workload runtime telemetry through integration with the Bank's EDR/XDR, SIEM and threat-intelligence platforms. The solution shall support ingestion of external threat-intelligence to enrich and prioritise workload findings."	No Change, Please be guided by the RFP
870	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 47 and S.No. 48	S.No. 47 - The solution shall support high availability and service continuity appropriate to the proposed deployment architecture and shall provide mechanisms for recovery of relevant configurations and security policies. S.No. 48 - The solution shall provide mechanisms to identify the protection health/status of onboarded workloads, including agent, connector or communication health where applicable.	For OEM-managed SaaS delivery, high availability, redundancy and disaster recovery are provided within the OEM platform under its published availability SLA and cannot be operated or restored by the Bank. We request you to kindly ammend S.No. 47 as following - "For SaaS-delivered solutions, the OEM shall provide high availability, redundancy and disaster recovery within the platform in line with its published availability SLA and shall provide mechanisms for export/retrieval of relevant configurations and security policies. For on-premises components, if any, the solution shall support HA and documented backup-restore." For S.No. 48, we request confirmation that reporting of connector/cloud-account onboarding and assessment health (and agent health only where an agent is proposed) shall be treated as compliant.	S.No. 47 - Please refer addendum for revised clause Clarification S.No. 48 - Bidder to propose the aproach ensuring the compliance with the sought requirement. Reporting of connector/cloud-account onboarding and assessment health shall also be considered compliant. Agent health reporting shall apply only where an agent is proposed/deployed.
871	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 49	The solution shall support consumption and correlation of relevant vulnerability, SBOM, CBOM and threat-intelligence information from the Bank's separately procured security solutions through APIs, supported integrations or equivalent mechanisms, where technically supported.	Consumption of Cryptographic Bill of Materials (CBOM) is an emerging requirement with no single established interchange standard, and correlation is only feasible if the source system and format are known. We request you to kindly confirm (a) the source solutions and the exact formats/standards in which SBOM and CBOM will be provided by the Bank (e.g., CycloneDX, SPDX and version), and (b) that where a standard format/API is not made available by the source solution, non-availability of such correlation shall not be treated as non-compliance, consistent with the qualifier 'where technically supported' in the clause.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
872	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM - Section scope (S.No. 1 to 69 and TOTAL MARKS 690)	Continuous Threat Exposure Management (CTEM) - all functional specifications, S.No. 1 to 69, TOTAL MARKS 690.	A significant proportion of the CTEM section (illustratively S.No. 1, 2, 5, 7 to 13, 18 to 23, 35, 55, 56, 57 and 67) specifies Cyber Threat Intelligence (CTI) and Digital Risk Protection (DRP) service deliverables - multilingual dark-web collection and translation, analyst-authored periodic and ad-hoc research reports, VIP investigation reports, threat-actor dossiers and engagement with threat actors, compromised-credential and payment-card monitoring, takedown/reporting to external authorities, named analyst and incident-response services. These are analyst-delivered managed services and are distinct from a Continuous Threat Exposure Management platform, which (per the recognised CTEM framework) delivers scoping, discovery, prioritisation, validation and mobilisation of exposures across the attack surface. As currently drafted, the section can be fully met only by DRP/CTI service providers and is restrictive to exposure-management platform OEMs, even though the Bank has separately (at VA-VM S.No. 87 and 88) contemplated CTEM as the platform that consolidates and prioritises findings across scanning engines. We therefore request you to kindly split this section into (a) 'CTEM / Exposure Management Platform' and (b) 'Cyber Threat Intelligence and Digital Risk Protection Services', with separate functional specifications, separate marks and separate	No Change, Please be guided by the RFP
873	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 1, S.No. 2 and S.No. 7	S.No. 1 - The solution should collect intelligence from multiple languages and relevant regional sources, with support for multilingual threat intelligence processing and analysis. S.No. 2 - The solution should support translation or interpretation of collected intelligence into English. S.No. 7 - Each intelligence item should include metadata such as date, author, source, and pre-classification of raw data.	Multilingual collection from closed/regional sources, machine translation of collected raw intelligence, and 'author'-level metadata with pre-classification of raw data are characteristics of a dark-web/DRP collection platform and are not features of a CTEM/exposure management platform. We request you to kindly move these clauses to the proposed Cyber Threat Intelligence/DRP service scope. If they are retained under CTEM, We request you to kindly ammend them as following - "The solution shall provide vulnerability, exploit and exposure intelligence in English, with source, publication date and classification metadata, and shall support ingestion of multilingual/regional intelligence from bank-approved third-party sources through supported integration mechanisms."	Please refer addendum for the revised clause
874	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 8 and S.No. 53	S.No. 8 - The solution should allow messaging and collaboration within the context of a specific intelligence item. S.No. 53 - Each alert should include a discussion board for eligible users to collaborate within the alert context.	An in-product messaging/discussion board is a vendor-specific user-interface feature, and for a bank, collaboration and audit trails on security findings are better retained in the Bank's ITSM/SOAR system of record rather than in a third-party SaaS console. We request you to kindly consider the change in the clause - "The solution shall support collaboration on a specific exposure, alert or intelligence item through comments/annotations, assignment and status tracking within the platform and/or through bidirectional integration with the Bank's ITSM/SOAR/ticketing platform."	No Change, Please be guided by the RFP
875	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 9	The solution shall provide access to proprietary, internally generated, licensed or equivalent high-quality threat intelligence sources capable of providing actionable intelligence relevant to the Bank's environment.	We request confirmation of the nature of intelligence expected. Exposure-management OEMs provide proprietary research-generated vulnerability, exploit and exposure intelligence (including exploit availability, exploitation-in-the-wild, ransomware association and predictive exploitability), whereas dark-web/actor intelligence is sourced by DRP providers. We request you to kindly consider the change in the clause - "The solution shall provide access to the OEM's proprietary/internally generated and/or licensed intelligence covering vulnerabilities, exploits, exploitation activity and exposures relevant to the Bank's environment, and shall support ingestion of additional bank-approved third-party intelligence sources."	No Change, Please be guided by the RFP
876	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 10	Analysts should perform threat hunting activities to find findings outside of the platform.	This clause requires a human analyst-delivered managed service and is not a functional specification of a solution. Scoring it within a functional compliance sheet at 10 marks does not permit objective evaluation. We request you to kindly move this clause to the managed services/MSSP or CTI service scope of the RFP with defined service levels (number of analyst hours, hunting frequency, deliverable and reporting format) and a separate commercial line item, so that bidders can price it objectively. If it is retained, kindly define the expected analyst effort and deliverables.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
877	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 11	The solution/service should generate investigation reports for designated VIPs or other high-risk identities/assets, providing an overview of identified digital exposure and associated risk.	VIP/executive digital exposure investigation is a Digital Risk Protection service deliverable involving collection of personal digital footprint data, and carries data-protection considerations under the DPDP Act for the named individuals. We request you to kindly move this clause to the Cyber Threat Intelligence/DRP service scope. If retained, kindly confirm the number of designated VIPs/high-risk identities, the frequency of such reports and the consent/lawful-basis framework the Bank will provide for processing their personal data, so that bidders can price and lawfully deliver the service.	No Change, Please be guided by the RFP
878	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 5, S.No. 12 and S.No. 13	S.No. 5 - automated and/or AI-assisted generation of tailored intelligence reports based on customer requirements. S.No. 12 - general and industry-related cyber intelligence reports on threat landscape trends, at least twice a month. S.No. 13 - the solution should be able to commission ad-hoc research reports on demand.	Periodic (twice monthly) industry threat-landscape reports and ad-hoc commissioned research reports are analyst-authored service deliverables, and 'on demand' without a defined ceiling is commercially open-ended. We request you to kindly move these clauses to the Cyber Threat Intelligence service scope with defined deliverables, and kindly confirm (a) the maximum number of ad-hoc research reports that may be commissioned per annum, (b) the expected turnaround time, and (c) whether these are to be priced within the platform subscription or as a separate service line item.	a. Periodic industry threat-landscape reports - At least a month b. Ad-hoc commissioned research reports: The requirement shall shall relate to threats, exposures, vulnerabilities and risk areas relevant to the Bank c. Bidder to ensure that all requite cost is factored and the requirement is complied at not additional to the bank Please refer addendum for revised clause
879	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 18	The solution should provide comprehensive threat actor attribution including known identities, motivations, historical activity, TTPs, associated infrastructure, and MITRE ATT&CK mapping.	Threat-actor attribution dossiers covering actor identities, motivations and associated infrastructure are CTI/DRP deliverables. Exposure-management platforms provide threat-actor and campaign context mapped to MITRE ATT&CK for the vulnerabilities and exposures identified in the Bank's environment. We request you to kindly move this clause to the Cyber Threat Intelligence service scope, or update it as following - "The solution shall provide threat context for identified exposures, including associated threat actors/campaigns, observed exploitation activity, TTPs and MITRE ATT&CK mapping, where such intelligence is available, and shall support enrichment from bank-approved third-party threat-intelligence sources."	Please refer addendum for revised clause
880	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 19	The solution should detect compromised credentials for employees and VIPs, exposed payment card information, and aggregate data from known breach databases in real time	Detection of compromised credentials and exposed payment-card data through aggregation of breach and dark-web databases is a Digital Risk Protection capability and requires the provider to collect, store and process the Bank's employees' and customers' personal and card data, with attendant DPDP Act and PCI DSS implications. We request you to kindly move this clause to the Cyber Threat Intelligence/DRP service scope of the RFP. If retained under CTEM, kindly confirm the employee/identity count and card-BIN ranges to be monitored, and the data-processing and retention framework the Bank will mandate for such personal and cardholder data.	Please refer addendum for revised clause
881	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 21	The solution should support threat actor interaction via vendor analysts (e.g., engaging via dark web avatars) to gather additional intelligence	Engagement with threat actors through covert dark-web personas is offered by a very small number of DRP providers, cannot be objectively evidenced or evaluated in a technical compliance sheet, and exposes a regulated bank to legal, reputational and regulatory risk arising from interaction with criminal actors on its behalf. We request you to kindly reconsider this clause from the CTEM functional specifications, as it is restrictive to a limited set of vendors and is not required to achieve continuous threat exposure management outcomes. If the Bank wishes to retain such capability, we request it be moved to an optional service line item, excluded from the technical scoring.	Please refer addendum for the revised clause
882	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 23	The solution should support reporting of confirmed malicious or phishing assets to relevant external platforms and authorities, where such reporting is supported and authorized.	Reporting and takedown of malicious/phishing domains and assets with registrars, hosting providers, app stores and authorities is an anti-phishing/brand-protection service, delivered under authorisation letters from the brand owner. We request you to kindly move this clause to the anti-phishing/brand protection service scope. If retained, kindly confirm the expected number of takedown/reporting requests per annum and the applicable turnaround SLA, and confirm that the Bank will provide the requisite authorisation to act on its behalf, so that bidders can price the service.	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
883	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 20, 22, 45 and 47	S.No. 20 - IoC enrichment allowing submission of IPs, domains and hashes to receive contextual threat intelligence and threat actor attribution; S.No. 22 - scanning and reputation analysis of submitted IP addresses; S.No. 45 - manual IoC management operations; S.No. 47 - cross-platform IoC enforcement across the security stack.	IoC submission, enrichment, lifecycle management and - in particular - enforcement of IoCs across the security stack are functions of a Threat Intelligence Platform (TIP) and SOAR, both of which are in scope of this RFP. Enforcement (pushing blocklists to NGFW, proxy, DNS, EDR and email gateways) is performed by those controls under the Bank's change-management process, not by an exposure-management platform. We request you to kindly move S.No. 45 and S.No. 47 to the TIP/SOAR scope, and update S.No. 20 and S.No. 22 as following - "The solution shall support enrichment of submitted indicators (IP addresses, domains, hashes) with available contextual intelligence and reputation information natively and/or through integration with the Bank's threat-intelligence platform, and shall support publishing of validated indicators to the Bank's security controls through the Bank's SOAR/TIP."	Please refer addendum for the revised clause
884	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 24	The solution should provide pre-built bidirectional integrations with SIEM, SOAR, ticketing (Manage Engine), and threat intelligence platforms	Availability of a 'pre-built' connector is vendor-specific, whereas equivalent bidirectional integration is routinely achieved through documented REST APIs and webhooks with the same functional outcome. We request you to kindly share the Vendor/Model/Version of the SIEM, SOAR, ManageEngine ticketing product and threat-intelligence platform to be integrated, and update the clause as following - "The solution shall provide bidirectional integration with the Bank's SIEM, SOAR, ticketing (ManageEngine) and threat-intelligence platforms through pre-built connectors, documented REST APIs, webhooks or equivalent mechanisms."	Please refer addendum for the revised clause
885	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 30 and S.No. 33	S.No. 30 - The solution shall provide automated validation of identified exposures, where technically applicable and authorized by the Bank, using controlled, non-destructive testing or equivalent validation mechanisms to determine whether the identified exposure is genuinely exploitable or materially exposed. S.No. 33 - The solution should validate that a vulnerability is actually exploitable or otherwise materially exposed (active exposure validation).	Active, automated exploitation-based validation of findings is the function of Breach and Attack Simulation (BAS) or automated penetration-testing tooling - which the Bank itself references at S.No. 41 of this section as a separate external source to be integrated. Exposure-management platforms establish material exposure and exploitability through evidence-based validation: authenticated/unauthenticated verification of the finding, reachability and internet-exposure analysis, attack-path analysis, exploit availability and exploitation-in-the-wild intelligence. We request you to please consider a below change: "The solution shall validate whether an identified exposure is genuinely exploitable or materially exposed using evidence-based validation - including verification of the finding, internet exposure and network reachability analysis, attack-path analysis, exploit availability and observed exploitation intelligence - and shall support ingestion of validation results from the Bank's BAS/penetration-testing tools through supported integration." Kindly also confirm that active exploitation testing against the Bank's production environment is not mandated as a day #1 platform capability.	Please refer addendum for the revised clause
886	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 35	The solution should detect malicious files, reconnaissance activity, automated attack tools, and target lists	Detection of reconnaissance activity, automated attack tooling and 'target lists' naming the Bank requires deception/honeypot sensors, network detection telemetry or dark-web collection, none of which are capabilities of a CTEM/exposure management platform. We request you to kindly reconsider this clause from the CTEM section (reconnaissance and attack-tool detection being already addressed by the Bank's NDR, WAF, NGFW and SOC/SIEM scope), or move it to the Cyber Threat Intelligence/DRP service scope.	Please refer addendum for the revised clause
887	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 41	The solution should support external vulnerability source integrations such as VA/VM scanners, ASM, XDR, BAS, Dark Web Monitoring, and MDM/UEM	Integration is feasible only where the source product, version and API are known, and Dark Web Monitoring and BAS are separate product categories which the Bank may or may not have licensed. We request you to kindly (a) share the Vendor/Model/Version of each source solution to be integrated (VA/VM, ASM, XDR, BAS, Dark Web Monitoring, MDM/UEM), (b) confirm which of these the Bank already owns and which are expected to be supplied by the bidder, and (c) confirm that non-availability of integration with a product the Bank has not licensed, or which does not expose a supported API, shall not be treated as non-compliance.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
888	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 42 and S.No. 43	S.No. 42 - The solution should use machine learning to evaluate the business impact of each remediation action and prioritize high-priority exposures S.No. 43 - The ML model should continuously study the environment including asset relationships, topology, and security controls to detect false positives and identify root causes.	These clauses mandate a specific implementation mechanism ('machine learning', 'the ML model') and a specific analytic behaviour rather than the security outcome, which is restrictive to a particular OEM's product design. The Bank has adopted a technology-neutral formulation elsewhere in this very section (S.No. 34 - 'using AI/ML or equivalent analytic'). We request you to kindly change the clause, consistent with S.No. 34 - "The solution shall prioritise exposures using AI/ML or equivalent analytics based on asset criticality and business context, exploitability, exposure, asset relationships/topology and the effect of existing security controls, and shall support identification of false positives and of common root causes to enable efficient remediation."	No Change, Please be guided by the RFP
889	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 38 read with S.No. 41 and S.No. 48	S.No. 38 - The solution should be deployed agentlessly, without requiring sensors or agents on endpoints, servers, or network appliances. S.No. 41 - external vulnerability source integrations such as VA/VM scanners, ASM, XDR, BAS, Dark Web Monitoring, and MDM/UEM. S.No. 48 - The solution should assess and harden network, endpoint, and operating system security controls.	S.No. 38 mandates a fully agentless and sensor-less deployment, while S.No. 48 requires assessment and hardening of endpoint and operating-system security controls - which requires either a credentialed/authenticated scan, an agent, or ingestion from the agent-based VA/VM, XDR and MDM/UEM platforms referenced in S.No. 41. These clauses partially contradict each other. We request you to kindly confirm that the CTEM platform itself may remain agentless and derive endpoint/OS control assessment through integration with the Bank's VA/VM, XDR and MDM/UEM platforms and credentialed configuration audit performed by those tools, and kindly update S.No. 48 as following - "The solution shall consolidate and report on the configuration/hardening posture of network, endpoint and operating system security controls, natively and/or by ingesting configuration and compliance assessment results from the Bank's VA/VM, XDR, MDM/UEM and related platforms."	Please refer addendum for the revised clause
890	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 49 and S.No. 50	S.No. 49 - The solution should provide a private exposure map of the organization's attack surface. S.No. 50 - The solution should support custom protections tailored to the organization's environment.	The terms 'private exposure map' and 'custom protections' are vendor-specific product terminology and are not objectively evaluable; 'protections' further implies enforcement, which a CTEM platform does not perform. We request you to kindly change the clause - S.No. 49 - "The solution shall provide a consolidated, access-controlled map/inventory of the organisation's internal and internet-facing attack surface, including assets, relationships, exposures and attack paths." S.No. 50 - "The solution shall support custom policies, custom detection/assessment rules, custom risk scoring and custom tagging tailored to the organisation's environment."	S.No 49.: Please refer addendum for revised clause Clarification: S.No 50: " & M500
891	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 51, 59, 60, 62 and 63	S.No. 51 - apply virtual patching/ compensating controls/exposure mitigation mechanism to the firewall and other security systems through integration with relevant security controls; S.No. 59 - API-based remediation, notification or workflow integration with relevant security controls; S.No. 60 - automated remediation workflows; S.No. 62 - leverage compensating controls and layered defense strategies; S.No. 63 - collaboration tools and ITSM integration for remediation workflows.	These clauses require the CTEM platform to execute configuration changes directly on the Bank's production security controls (firewall, WAF, IPS, EDR). In a regulated banking environment such changes must pass through the Bank's change-management and maker-checker controls, and the accountable system of record for orchestration is the Bank's SOAR/ITSM, which is separately in scope under this RFP. We request you to kindly change the clause - "The solution shall identify applicable compensating controls, virtual patching and exposure-mitigation options for identified exposures, shall provide the corresponding remediation/mitigation instructions and artefacts, and shall trigger and track remediation through API/webhook-based integration with the Bank's SOAR, ITSM and relevant security controls. Actual enforcement of changes on production security controls shall be performed by the respective control through the Bank's approved change-management process." Kindly confirm that compliance achieved through such SOAR/ITSM-orchestrated remediation shall not be treated as non-compliance.	Please refer addendum for revised clause Clarification: S.No 63: No Change, Please be guided by the RFP.
892	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 61	The solution should ensure remediation actions do not disrupt business continuity	A security platform can assess and present the potential impact of a recommended remediation, but it cannot guarantee the business-continuity outcome of a change executed on the Bank's production systems, which depends on the Bank's change-management, testing and rollback processes and on the affected application's architecture. As worded, the clause places an unqualified guarantee on the bidder/OEM. We request you to kindly ammend the clause as following - "The solution shall provide impact assessment and risk context for recommended remediation actions, including affected assets, dependencies, prerequisites and rollback considerations, to enable the Bank to plan and execute remediation without disrupting business continuity through its change-management process."	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
893	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 55 and S.No. 56	S.No. 55 - The solution should include IOC investigation, infrastructure mapping, and threat actor identification. S.No. 56 - The visual investigation tool should integrate multiple services including WHO IS and Passive DNS.	A graph-based 'visual investigation tool' bundling WHOIS, Passive DNS and threat-actor identification is a specific feature of certain CTI/DRP investigation products and is not a CTEM platform capability; it is also available to the Bank through its threat-intelligence platform in scope under this RFP. We request you to kindly move these clauses to the Cyber Threat Intelligence/DRP or TIP scope, or update them as following - "The solution shall support investigation of identified exposures and indicators, including mapping of the Bank's internet-facing infrastructure and associated relationships (such as domains, sub-domains, certificates, DNS and WHOIS/registration data for the Bank's own digital footprint), and shall support enrichment and threat-actor context through integration with the Bank's threat-intelligence platform."	No Change, Please be guided by the RFP
894	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 57, S.No. 58 and S.No. 67	S.No. 57 - Up on demand, the vendor should provide a dedicated Customer Success Manager as a single point of contact for onboarding and ongoing support. S.No. 58 - The vendor to provide 24/7 system support. S.No. 67 - The vendor to provide a mechanism to report security incidents identified through the platform and receive prompt response and guidance from the incident response team.	These are commercial/service clauses rather than functional specifications of the solution, and 'dedicated Customer Success Manager' and access to an 'incident response team' are named-resource and incident-response-retainer commitments that cannot be objectively evaluated in a functional compliance sheet or priced without defined limits. We request you to kindly move these clauses to the services/SLA section of the RFP and confirm - (a) whether the Customer Success Manager is required to be dedicated to the Bank full-time or is an assigned named point of contact, and whether onsite presence is expected; (b) the required support SLA and severity-wise response/resolution matrix for 24/7 support; and (c) for S.No. 67, the number of incident-response engagements per annum, whether remote or onsite, and whether these are to be priced within the subscription or as a separate retainer.	No Change, Please be guided by the RFP
895	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 65 and S.No. 66	S.No. 65 - The solution should aim to reduce Mean Time to Remediate (MTTR) and labor costs. S.No. 66 - The solution should maximize ROI from existing security tools by optimizing the security posture.	These clauses express desired business outcomes rather than verifiable functional specifications, and each carries 10 marks in a scored technical compliance sheet. Compliance cannot be objectively demonstrated or evaluated, and every bidder will necessarily mark itself compliant, which adds no discriminatory value to the Bank's evaluation. We request you to kindly either reconsider these clauses from the scored functional specifications, or replace them with measurable requirements as following - S.No. 65 - "The solution shall provide MTTR measurement and trending for exposures by severity, asset criticality and business unit, including SLA tracking and ageing analysis." S.No. 66 - "The solution shall provide coverage and control-effectiveness reporting across the Bank's existing security tools, identifying assets not covered by, or gaps in, existing security controls."	Please refer addendum for revised clause
896	49	7.3.11 Cloud Security (CSPM) Tool		7.3.11 (Preamble) - Integrated cloud security solution providing a centralized and unified single-pane-of-glass view across all cloud assets, workloads, identities, configurations, applications, containers, AI services and cloud-native resources deployed across multi-cloud, hybrid-cloud and on-premises environments.	Unified visibility across cloud assets, workloads, identities, configurations, containers, Kubernetes, AI services and cloud-native resources across multi-cloud and hybrid-cloud is met from a single console. Deviation: 'on-premises environments' - CSPM assesses cloud provider control planes through APIs and has no control plane to assess for traditional on-premises infrastructure. On-premises posture is delivered through configuration/compliance benchmark auditing in the VA & VLM solution, and on-premises Kubernetes through the cloud security platform. Request the Bank confirm that on-premises security posture assessed via CIS/benchmark configuration audit in the VA & VLM solution, consolidated into the same single pane, is acceptable.	No Change, Please be guided by the RFP
897	50	7.3.11 Cloud Security (CSPM) Tool		7.3.11.2 (10) - Key Deliverable: Incident Response & Automated Playbooks.	The platform provides prioritized findings, remediation guidance, auto-generated remediation code (IaC/CLI), and event/webhook/API triggers that drive downstream automation. Deviation: incident response playbook authoring and execution is SOAR functionality, and SOAR is separately in scope under this RFP. The CSPM tool cannot itself be the playbook execution engine. Request the Bank confirm that this deliverable will be met by publishing CSPM findings and triggers into the Bank's SOAR/ITSM, with the response playbooks built and executed there.	No Change, Please be guided by the RFP
898	51	7.3.11 Cloud Security (CSPM) Tool		7.3.11.2 (12) - Ensure that the reports are extracted from online / warehouse storage etc. Restore the logs/data from backup for forensic investigation and as per bank requirement without any additional cost.	Findings, assessment history, audit logs and reports are retrievable on demand through the console, scheduled reports and APIs at no additional cost for the retention period applicable to the subscription. Deviation: for an OEM-managed SaaS platform there is no Bank-accessible backup media from which data is 'restored'; data is served from the live platform and its retention tier. Request the Bank (a) specify the mandated retention period, and (b) accept on-demand retrieval/export from the platform as fulfilling this requirement.	Please refer the addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
899		APPENDIX 1A Functional Compliance Sheet (Solutions), Page 23	Point 18	The proposed solution shall provide cloud-native high availability and redundancy mechanisms to tolerate failures of underlying infrastructure components without disruption to security monitoring and operational capabilities. The solution shall provide automated failover and service continuity within the cloud environment through the CSP's native availability and resiliency capabilities	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. "" The proposed solution shall provide cloud-native redundancy mechanisms to tolerate failures of underlying infrastructure components without disruption to security monitoring and operational capabilities. The solution shall provide automated failover and service continuity "	Please refer the addendum for revised clause
900	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 23	XSIAM	Point 36	The proposed solution must come with out-of the-box/customized to be delivered on day 1 support integration and dashboards, reports, rules etc. to provides rapid insights and operational visibility into large-scale CentOS, Windows, Unix and Linux environments machine data.: syslog, metrics and configuration files.	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""The proposed solution must come with out-of the-box/customized to be delivered on day 1 support integration and dashboards, reports, rules etc. to provides rapid insights and operational visibility into large-scale CentOS, Windows, Linux environments machine data.: syslog, metrics and configuration files.	No Change, Please be guided by the RFP
901	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 24	XSIAM	Point 59	The proposed solution machine learning capabilities must allow addition or have inbuilt feature of custom machine learning algorithms from popular open-source libraries like NLP, Python etc.	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""The proposed solution must natively supports custom machine learning algorithms through its built-in Bring Your Own Machine Learning (BYOML) framework. This capability allows mature Security Operations Centers (SOCs) and security data scientists to access the massive security data lake stored within the platform and run bespoke analytics tailored to their specific environment.	No Change, Please be guided by the RFP
902	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 37	XDR	Point 43	The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature or through seamless integration with a third-party sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature or through seamless integration with a third-party sandboxing solution from day 1.""	Please refer the addendum for revised clause
903	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 1.4	Identity Threat Detection Solution must find and present high-risk attack pathways to critical IT assets	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. "ITDR provides identity risk context through User Risk View, Risk Management Dashboard, and identity alerts.	Please refer the addendum for revised clause
904	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 1.6	Identity Threat Detection Solution should must automatically prioritize and remediate the riskiest identities to preemptively cut off what attackers need (and expect to find) to move undetected within the network.	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. "ITDR identifies risky identities and supports remediation workflows for suspicious identity activity."	Please refer the addendum for revised clause
905	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.3	The ITDR solution shall identify and assess exposed, improperly stored, or compromised credentials associated with user, privileged, service, and administrative identities on endpoints	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ITDR identifies risky identity posture, weak or compromised credentials, and suspicious activity involving user, privileged, service, and administrative accounts.	Please refer the addendum for revised clause
906	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.4	Identity Threat Detection Solution should Identify, Misconfigured accounts, Legacy app accounts, Stale accounts, password policy violations, Kerberoastable credentials, unmanaged user accounts, unmanaged service accounts	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""ITDR identifies risky identity posture, weak or compromised credentials, Kerberoasting activity, and suspicious behavior involving service and administrative accounts""	Please refer the addendum for revised clause
907	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.5	Identity Threat Detection Solution should Provide continuous monitoring and customizable, automated business rules to eliminate security policy violations, such as: • Stored credentials to sensitive assets • Local-admin accounts • Cached credentials stored in browsers, Windows and other systems	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""ITDR continuously monitors identity posture and access relationships to identify risky configurations, excessive privileges, and suspicious identity activity across Active Directory and related identity sources.""	Please refer the addendum for revised clause
908	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.7	Identity Threat Detection Solution should be available through rack-mountable on-premise deployment	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""Identity Threat Detection Solution should be available through rack-mountable on-premise deployment not applicable for SaaS solution ""	Please refer the addendum for revised clause
909	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.9	Identity Threat Detection Solution should detect all types of attack vectors including but not limited to pre attack reconnaissance,zero- day attacks, privilege escalation prevention, lateral movement, data theft	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""ITDR detects identity-based threats such as Active Directory reconnaissance, compromised accounts, privilege escalation, and anomalous access, while providing identity context to help investigate exposure and attack paths.""	The Clause is applicable only to idendity related threat vector only. The volumetrics is provided in the RFP and should be complied

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
910	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.15	Identity Threat Detection controls should be able to automatically discover and flag hidden or shadow Tier 0 assets	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""Identity Threat Detection and Response helps identify risky identity assets, excessive privileges, and exposure across identity relationships.""	Please refer the addendum for revised clause
911	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.17	Identity Threat Detection Solution should be able to pull and analyze identity data from AD, Entra ID, identity stores, PAM systems	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""ITDR analyzes identity data from supported identity sources, including Active Directory and Microsoft Entra ID, to provide context on identities, permissions, and access exposure""	Please refer the addendum for revised clause
912	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 3.4	The Identity Threat Detection Solution should integrate with compatible endpoint/extended detection solution to capture screen recordings or screenshots during active attacker sessions, as part of advanced forensic evidence collection	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""ITDR integrates with supported tools to share identity and endpoint context for investigation and response, including forensic collection where available.""	Please refer the addendum for revised clause
913	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 3.5	The Identity Threat Detection Solution should integrate with compatible network detection solution to support collection of PCAP data to support network-level visibility of the incident	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""ITDR integrates with supported tools to share identity risk context and support investigation workflows, including network-related telemetry where available.""	Please refer the addendum for revised clause
914	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 53	ITDR	Point 3.7	Identity Threat Detection Solution should, as part of its forensic data collection process, include detailed attack path information, including the protocols leveraged during the attack.	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""ITDR provides identity context through asset, permission, and authentication analysis, and detects identity-based threats such as compromised accounts, privilege escalation, anomalous access, and Active Directory reconnaissance.""	Please refer the addendum for revised clause
915	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 53	ITDR	Point 3.9	Identity Threat Detection solution should detect an adversary's attempt to move laterally toward the organization's key assets using as many hosts (Windows, Mac, or Linux) as possible in the organization without requiring a persistent agent.	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""Identity Threat Detection solution should detect an adversary's attempt to move laterally toward the organization's key assets using as many hosts (Windows, Mac, or Linux) as possible in the organization With or without requiring a persistent agent.""	Please refer the addendum for revised clause
916	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 53	ITDR	Point 3.10	Identity Threat Detection Solution should collect user and computer information from Active Directory as part of its forensic data gathering to enhance context and assess risk exposure. detect at the earliest point in the attack, post initial compromise as the attacker is first attempting to move laterally and escalate privilege.	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""ITDR collects and analyzes identity data to improve context and assess risk exposure. It detects identity-based threats, including compromised accounts, privilege escalation, anomalous access, and Active Directory reconnaissance, early in the attack path.""	Please refer the addendum for revised clause
917	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 53	ITDR	Point 3.11	Identity Threat Detection Solution should collect user and computer data from Active Directory during forensic data gathering to improve context and evaluate risk exposure, while ensuring that all deception techniques remain hidden from legitimate users.	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""Identity Threat Detection and Response collects and analyzes identity data to improve context and assess risk exposure. It provides deep visibility into identity assets, permissions, relationships, and authentication activity across Active Directory and other identity sources. ITDR also supports forensic investigations through endpoint data collection and analysis."	Please refer the addendum for revised clause
918	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 19	CTEM	Point 7	Each intelligence item should include metadata such as date, author, source, and pre-classification of raw data	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""Intelligence items include enriched context, source information, and analysis metadata to support investigation and prioritization.""	Please refer the addendum for revised clause
919	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 19	CTEM	Point 11	The solution/service should generate investigation reports for designated VIPs or other high-risk identities/assets, providing an overview of identified digital exposure and associated risk.	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""The solution provides risk context and investigation views for identities and assets, helping analysts assess exposure and related risks.""	No Change, Please be guided by the RFP
920	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 20	CTEM	Point 38	The solution should be deployed agentlessly, without requiring sensors or agents on endpoints, servers, or network appliances	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""The solution should be deployed agentlessly, With or without requiring sensors or agents on endpoints, servers, or network appliances""	Please refer the addendum for revised clause
921	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 81	ASM	Point 6	The visual representations should be downloadable in PDF, JPG, PNG and other generally used formats	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""The solution supports exporting reports and data views in supported file formats such as PDF, CSV, TSV, JSON, or ZIP, depending on the workflow""	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
922	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 81	ASM	Point 8	The solution shall provide information on vulnerabilities, misconfigurations, insecure configurations, obsolete or unsupported technologies, applications, services, URLs, ports, network components, systems, databases and other relevant infrastructure that are publicly exposed or otherwise identifiable through authorized discovery and assessment activities.	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""The solution provides exposure information for internet-facing assets, including vulnerabilities, misconfigurations, services, and related attribution data discovered through authorized asset mapping and assessment.""	Please refer addendum for revised clause
923	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 81	ASM	Point 9	The solution should provide data/information on security flaws/ inherent vulnerabilities (allegedly) reported about the digital products exposed to the Internet (For example: internet banking, mobile applications) offered to the bank's customers, as leaked in public domain, or other forums	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""The solution provides exposure and risk information for internet-facing digital assets, including vulnerabilities, services.""	No Change, Please be guided by the RFP The requirement is intended to provide visibility not only into directly identified technical vulnerabilities but also into relevant security information concerning the Bank's internet-facing digital products
924	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 81	ASM	Point 10	The solution shall identify and provide relevant information on potentially exposed sensitive information associated with the Bank, including source-code references, code snippets, API information, credentials, keys and other security-relevant information, where such information is identifiable through publicly available sources, external attack-surface intelligence or other authorized discovery mechanisms.	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""The solution provides exposure information for internet-facing assets, including vulnerabilities, misconfigurations, code weaknesses, and exposed secrets discovered through attack surface.""	Please refer addendum for revised clause
925	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 54	Cloud security	Point 4	The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud environment like AWS/Azure/GCP/Meghdoot, AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud environment like AWS/Azure/GCP/, AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.	Please refer the addendum for revised clause
926	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 55	Cloud security	Point 9 (Sub point)	○Automatic, in-product remediation via the Cloud Service Provider (CSP) API (1-click)	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""The solution supports in-product remediation workflows, including automated actions and approval-based playbooks where configured.	Please refer the addendum for revised clause
927	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 56	Cloud security	Point 25	The solution must provide an self-service portal for engineers. The admin portal should be able to define the eligibility for users and groups, based on role, scope and duration. The solution should provide approval workflow and audit logs	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation.'' The solution supports granular access control, human approval in select workflows, and audit logging for access-related changes.	Please refer the addendum for revised clause
928	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 40	NDR	Point 9	Easy-to-manage, clientless platform that deploys quickly and involves minimal or no dependency on customization and management.	We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. ""Easy-to-manage, clientbase clientless platform that deploys quickly and involves minimal or no dependency on customization and management.""	Please refer the addendum for revised clause
929	RFP Pg 35	Deployment Pattern	Point d	NDR: The NDR solution shall be deployed On-Premises within the Bank's DC and DR, with the required brokers, aggregators, collectors and/or enforcement components configured in N+N Active-Active configuration at both sites.	The proposed NDR solution shall utilize a hybrid deployment model or SaaS model.With the required brokers/ aggregators/collectors /Sensors and enforcement components configured in N+N Active-Active or Active- Passive configuration at both sites DC and DR.	Please refer addendum for the revised clause
930	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 40	NDR			Clarification: Kindly confirm the specific physical interface type and speed the Bank will provide for the uplink to the NDR sensor.	Details shall be shared with successful bidder
931	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 40	NDR	Point 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	"We request you to please consider the change in the clause as following. This modification will facilitate wider bidder participation. "" The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead.""	Please refer Addendum for revised clause
932	Page 68	7.7 On-cloud proposed solution OEM Responsibilities	Page 8	The solution shall support secure connectivity with the Bank's on-premises infrastructure,cloud environments, and external systems through private and secure communication mechanisms.	Few OEMs are a SaaS solution accessible over the internet using passwords and multi-factor authentication and Https. However, access to your SIEM tenant can be restricted based on your Bank's static public IP addresses. We request you to please consider the change in the clause as following "" The solution shall support secure connectivity with the Bank's on-premises infrastructure,cloud environments, and external systems through private or secure communication mechanisms via internet or tenant can be restricted based on Bank's static public IP addresses.."""	Please refer the addendum for revised clause
933	RFP Pg 33	Section 7.2.3 Deployment Model Definition		CSP-hosted components shall provide cloud-native High Availability (HA), geographic resiliency and DR in accordance with the SLA, RTO and RPO requirements specified in this RFP.	Few OEMs are pure SaaS Solution. Request you to please indly reconsider this for SaaS offerings.	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
934	RFP Pg 43	7.3.2.2 Key Deliverables	Point 7	Backup, retention, restoration, documentation and knowledge transfer for configured security automation capabilities and use cases.	Could you please provide provide information on this clause	No Change, Please be guided by the RFP Refer Section7.2.4.3 Storage and other Requirement
935	Appendix 1A Page 40	NDR Functional Compliance Sheet	Clause 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high- availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	The Clause mandates Cloud based SaaS model, while RFP Page 30, Page 35, section 7.2.4.1 clause 'd' asks for on Premesis solution "The NDR shall be deployed On-Premises". We request to modify the clause to include On-Prem solution also	Please refer Addendum for revised clause
936	Appendix 1A Page 40	NDR Functional Compliance Sheet	Clause 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high- availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	The Clause asks for Active-Active HA architecture, we request to include Active-Standby Mode. Justification: Management Console is central console, it cannot be deployed in Active-Active mode, as it is a central component.	Please refer Addendum for revised clause
937	Appendix 1A Page 41	NDR Functional Compliance Sheet	Clause 18	Solution should have the capabilities to create and run security playbooks for automation and better MTTD/MTTR on the basis of criticality of threat/server	Proposed solution adopts below appraoch for automated MTTD, Solution need investigative workflows and all the alerts need to be validated before building any Active Response Solution is having inbuilt playbooks like Host, Session and Packet analysis. once alert is validated Active Response can be triggered. Hope the approach is acceptable	Yes, your understanding is correct Also, Please refer addendum for the revised clause
938	Page 66	7.6.7	Training	At a minimum, the following training programs shall be conducted for each proposed solution / OEM appointed officials: Duration per Session and Munimum Number of Sessions	Overall there is a requirement of 15 Sessions and Duration per session is 2 or 3 days. This takes the total training per solution to 40 days. This is very large reqirement of training, we request to make it to 3 days for NDR solution	Please refer addendum for revised clause
939	Page 63	7.6.6	Testing, clause 3	The bidder shall provision and maintain dedicated Development, Testing, UAT, and Pre-Production environments throughout the contract period.	Is UAT Environment required for NDR solution also, given that NDR is a Passive and out of path solution.	Please refer addendum for revised clause
940		ITDR	1.7	Detect and respond to active threats with high fidelity (low false positives and false negatives).	Pre-Bid Query / Clarification: The Bank has separately specified a comprehensive deception platform for detection of active attacker activity, reconnaissance and lateral movement. We understand that the intent of this clause within ITDR is therefore to complement those controls with focused monitoring of the Bank's most critical identities. Considering that enhanced user-activity monitoring is most relevant for high-risk personnel such as executives, privileged users and other critical users, we request the Bank to kindly clarify whether this requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should provide high-fidelity detection and response for risky or anomalous user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, to identify activities associated with careless, malicious or compromised users.	No Change, Please be guided by the RFP
941		ITDR	1.8	Provide contextual information—who, what, when and how—to inform all stages of the attack chain.	Pre-Bid Query / Clarification: The Bank has already sought attack-lifecycle visibility under the separate deception requirements. For ITDR, we understand that additional value would be derived from detailed user-centric context for the Bank's most critical identities, enabling investigation of risky activity performed by such users. We request the Bank to kindly clarify whether this requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should provide contextual information—who, what, when, where and how—around risky user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, to support investigation and response.	No Change, Please be guided by the RFP
942		ITDR	1.9	Provide deep insights into both the potential and used privilege escalation and lateral movement steps in an attack.	Pre-Bid Query / Clarification: Privilege escalation and lateral-movement visibility is already substantially addressed under the separately specified deception solution, including attacker lifecycle visibility, MITRE ATT&CK mapping, deceptive attack paths and detection of lateral movement. To avoid duplication while retaining complementary investigation capability for high-risk identities, we request the Bank to kindly clarify whether this requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should provide deep insights into activities performed by up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, covering application usage, file and data movement, endpoint activity and other risky behaviours to support investigation of compromised, malicious or negligent user activity.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
943		ITDR	2.9	Detect all types of attack vectors including pre-attack reconnaissance, zero-day attacks, privilege escalation prevention, lateral movement and data theft.	Pre-Bid Query / Clarification: Pre-attack reconnaissance, lateral movement, malware/attack behaviour and attacker lifecycle visibility are already covered under the Bank's separate deception specifications. We understand that the complementary requirement under ITDR should focus on identity/user risk and potential data-loss activity for the Bank's most critical users rather than duplicate the deception control. We request the Bank to kindly clarify whether this requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should detect risky user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, including suspicious application usage, unauthorized access or movement of sensitive information, removable-media activity, web-based transfer, cloud synchronization and other potential data-exfiltration activities.	The Clause is applicable only to idendity related threat vector only. The volumetrics is provided in the RFP and should be complied
944		ITDR	2.10	Detect multiple attacks simultaneously.	Pre-Bid Query / Clarification: We understand the intent is to ensure that the solution is not restricted to investigation of a single event at a time. Since active attacker detection is separately covered by the deception solution, we request that this clause be clarified in terms of concurrent monitoring and investigation of risky activities across the Bank's designated critical-user population: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should be capable of detecting and investigating multiple risky user and data activities simultaneously across up to 100 critical/high-risk users and their monitored endpoints.	No Change, Please be guided by the RFP
945		ITDR	3.2	Provide unified presentation of both source- and target-based telemetry data in a timeline view.	Pre-Bid Query / Clarification: The Bank has separately specified end-to-end attacker visibility and behavioural analysis under the deception solution. For ITDR investigations involving critical identities, a chronological user-activity view would provide complementary evidence of actions performed by the user. We request the Bank to kindly clarify whether the requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should provide a unified chronological timeline of user- and endpoint-based activity telemetry for up to 100 critical/high-risk users identified by the Bank to support investigation of risky or suspicious user activity.	No Change, Please be guided by the RFP
946		ITDR	3.3	Correlate identity-related telemetry from relevant source and target systems to identify and investigate identity compromise, privilege escalation, credential abuse and lateral movement.	Pre-Bid Query / Clarification: Privilege escalation and lateral-movement detection are already addressed through the separately specified deception controls. To provide complementary investigation capability for the Bank's highest-risk identities, we request the Bank to clarify whether this clause may focus on correlation of user, endpoint, application and data activity for the designated critical-user population: Suggested Clarified Wording / Requested Action: The solution shall support correlation of user, endpoint, application and data-activity telemetry for up to 100 critical/high-risk users identified by the Bank to identify and investigate suspicious user behaviour, sensitive-data movement, policy violations and potential data-exfiltration activities.	No Change, Please be guided by the RFP
947		ITDR	3.4	Integrate with compatible endpoint/extended detection solution to capture screen recordings or screenshots during active attacker sessions as advanced forensic evidence.	Pre-Bid Query / Clarification: The Bank has separately specified attacker-session and forensic visibility through the deception platform. Within ITDR, we understand that visual evidence is intended to strengthen investigation of high-risk user activity. We request the Bank to kindly clarify whether the requirement may be read in an outcome-based manner for the designated critical-user population: Suggested Clarified Wording / Requested Action: The Identity Threat Detection Solution should support screenshots, screen capture or equivalent visual evidence of relevant activity for up to 100 critical/high-risk users during suspicious or high-risk user sessions, as part of forensic investigation and evidence collection.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
948		ITDR	3.5	Integrate with compatible network detection solution to support collection of PCAP data for network-level incident visibility.	Pre-Bid Query / Clarification: The requirement for PCAP is network-centric and does not directly relate to identity posture or focused user-activity monitoring. Further, the Bank's separate deception specifications already require high-interaction decoys, recording of attacker activities, traffic/behaviour visibility, forensic investigation and integration with network/security technologies. To avoid duplication of network-level forensic controls across two solution categories, we request the Bank to kindly delete this clause from the ITDR section. Suggested Clarified Wording / Requested Action: Requested action: Delete Clause 3.5 from the ITDR requirements, as equivalent/complementary network and attacker forensic visibility is already sought under the separate Deception requirements.	Please refer addendum for revised clause
949		ITDR	3.6	Push incident data into SIEM/XDR or SOAR technologies via integrations for improved incident management.	Pre-Bid Query / Clarification: We understand that the objective is to ensure relevant ITDR alerts and investigation context are available to the Bank's SOC ecosystem. For the enhanced monitoring of designated critical users, we request the Bank to kindly clarify whether alerts and activity information may be shared through supported integrations or APIs as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should make alerts and relevant incident/activity data for the monitored critical-user population available to SIEM/XDR, SOAR or other supported security platforms through integrations or APIs for improved incident management.	The proposed solution hould be integrated with SIEM/XDR or SOAR technologies for sharing the incident data via supported integrattion or APIs
950		ITDR	3.7	As part of forensic data collection, include detailed attack path information including protocols leveraged during the attack.	Pre-Bid Query / Clarification: Detailed attack-path and attacker-behaviour visibility is already sought under the separate deception specifications, including deceptive attack paths, MITRE ATT&CK mapping and forensic investigation. To avoid overlap while retaining complementary evidence for investigations involving the Bank's critical identities, we request the Bank to kindly clarify whether the requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should, as part of forensic data collection for up to 100 critical/high-risk users, include detailed user-activity information such as applications used, files accessed, data movement, destination channels and other relevant endpoint activity associated with the incident.	Please refer addendum for revised clause
951		ITDR	3.8	Collect user and computer information from Active Directory as part of forensic data gathering to enhance context and assess risk exposure.	Pre-Bid Query / Clarification: We understand that directory information is required to enrich investigations with user and computer context. We request the Bank to clarify that enterprise identity context may be maintained for the overall identity population, while detailed endpoint/user-activity telemetry may be applied to the Bank's designated critical-user population: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should use relevant user and computer identity information to enhance forensic context and risk assessment, and should correlate such context with detailed endpoint/user-activity telemetry for up to 100 critical/high-risk users identified by the Bank.	Please refer addendum for revised clause
952		ITDR	3.9	Detect an adversary's attempt to move laterally toward key assets using as many Windows, Mac or Linux hosts as possible without requiring a persistent agent.	Pre-Bid Query / Clarification: The Bank's separate deception specifications expressly require detection of lateral movement, reconnaissance, credential theft and malicious activity using agentless and/or agent-based deception techniques across the enterprise. The present clause therefore duplicates a capability already being procured under the Deception section. To avoid overlapping scope and duplicate controls, we request the Bank to kindly delete this clause from the ITDR section. Suggested Clarified Wording / Requested Action: Requested action: Delete Clause 3.9 from the ITDR requirements, since lateral-movement detection using deception techniques is already explicitly covered under the separate Deception specifications.	Please refer addendum for revised clause
953		ITDR	3.10	Collect AD user/computer information for forensic context and detect at the earliest point post initial compromise as the attacker first attempts lateral movement and privilege escalation.	Pre-Bid Query / Clarification: Early detection of lateral movement and privilege-escalation activity is substantially covered under the Bank's separate deception requirements. To retain a complementary identity/user-risk objective without duplicating the deception scope, we request the Bank to kindly clarify whether this clause may focus on early detection of risky activity among the designated critical-user population: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should use relevant identity context and detect risky user behaviour at the earliest possible point for up to 100 critical/high-risk users, based on monitored endpoint activities and configured detection policies, enabling investigation and response before such activity results in significant data loss or business impact.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
954		ITDR	3.11	Collect AD user/computer data during forensic gathering while ensuring all deception techniques remain hidden from legitimate users.	Pre-Bid Query / Clarification: The requirement to ensure deception techniques remain hidden from legitimate users is inherently a deception-platform capability. The Bank has already included comprehensive deception requirements covering lures, breadcrumbs, fake credentials, deceptive assets, attacker engagement and techniques designed to remain undetected by attackers. We therefore request the Bank to kindly delete this clause from the ITDR section to avoid duplication. Suggested Clarified Wording / Requested Action: Requested action: Delete Clause 3.11 from the ITDR requirements, as deception techniques and their concealment are already covered under the separate Deception specifications.	Please refer addendum for revised clause
955		Anti Phishing	17.1	Solution should detect at the earliest point in the attack, post initial compromise as the attacker is first attempting to move laterally and escalate privilege.	Pre-Bid Query / Clarification: Since this section is focused on Anti-Phishing, we understand that the objective is to identify suspicious activity following a successful phishing or account-compromise event. Network-level lateral movement and deception capabilities may be addressed by other security controls. We request the Bank to clarify whether this clause may instead focus on early post-compromise user activity visibility for the Bank's most critical users. Suggested Clarified Wording / Requested Action: The solution should support early identification and investigation of suspicious user activities associated with potential account compromise following phishing or other email-originated attacks, with enhanced user activity monitoring for up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles.	Please refer to the relevant Addendum for updated specfications
956		Anti Phishing	17.4	Solution must provide robust supply chain and AI/ML-driven contact chain analysis capabilities to identify and defend against socially engineered, impersonated, or BEC attacks.	Pre-Bid Query / Clarification: As compromise of trusted suppliers and partners is an important source of BEC and phishing risk, we request the Bank to clarify whether the existing supply-chain requirement should explicitly include behavioural analysis of supplier/partner communication patterns to identify attacks originating from compromised trusted accounts. Suggested Clarified Wording / Requested Action: Solution must provide robust supply-chain and AI/ML-driven contact-chain and behavioural analysis capabilities to identify and defend against socially engineered, impersonated or BEC attacks, including threats originating from compromised or impersonated supplier/partner accounts.	Please refer to the relevant Addendum for updated specfications
957		Anti Phishing	18	Solution must proactively analyze suspicious URLs using dynamic/behavioral analysis to prevent the spread of malware and other threats.	Pre-Bid Query / Clarification: The RFP separately addresses URL analysis and post-delivery remediation. We request clarification whether these requirements are intended to provide continuous protection throughout the email threat lifecycle, including pre-delivery analysis, click-time URL protection and post-delivery detection/remediation. Suggested Clarified Wording / Requested Action: Solution must provide continuous protection across the email threat lifecycle, including pre-delivery threat detection, real-time/click-time inspection of suspicious URLs, and post-delivery detection and automated remediation of threats that are subsequently determined to be malicious.	Please refer to the relevant Addendum for updated specfications
958		Anti Phishing	19.7	Solution must be able to offer a comprehensive portal that allows users to access information and metadata on events/incidents, facilitating network threat forensics for thorough investigation and analysis of potential security breaches or incidents.	Pre-Bid Query / Clarification: To strengthen investigation of phishing-led incidents involving executives and other critical users, we request clarification whether the existing forensic portal requirement may also include contextual user and endpoint activity for a limited population of Bank-identified critical/high-risk users. Suggested Clarified Wording / Requested Action: Solution must offer a comprehensive investigation portal providing information and metadata on events/incidents for forensic analysis. For up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, the portal should additionally provide contextual user and endpoint activity, including relevant application, file and user-action details, to support investigation of potential phishing-led compromise.	Please refer to the relevant Addendum for updated specfications
959		Anti Phishing	19.9	Solution must empower security operations and incident responders to automate the identification, remediation, and sharing of phishing threats, streamlining the process of detecting, addressing, and disseminating information about potential phishing attacks for improved response and mitigation.	Pre-Bid Query / Clarification: To improve SOC investigation efficiency, we request clarification whether the existing phishing identification and remediation requirement should include centralized attack context showing why a message was identified as malicious, the users targeted, associated threat indicators and remediation status. Suggested Clarified Wording / Requested Action: Solution must empower security operations and incident responders to automate identification, investigation, remediation and sharing of phishing threats, and should provide centralized contextual visibility into the users targeted, associated threat indicators, detection rationale, attack characteristics and remediation actions.	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
960		Anti Phishing	19.1	Solution must provide incident responders with real-time analytics and visibility into email-based attacks targeting the organization.	Pre-Bid Query / Clarification: Email-based attacks against executives and privileged users may require additional context after delivery to determine whether a targeted user has subsequently performed suspicious activity. We request the Bank to clarify whether real-time investigation visibility may include relevant user activity context for up to 100 Bank-identified critical/high-risk users. Suggested Clarified Wording / Requested Action: Solution must provide incident responders with real-time analytics and visibility into email-based attacks targeting the organization. For up to 100 Bank-identified critical/high-risk users, the solution should additionally provide contextual visibility into suspicious user activities associated with potential phishing or account compromise, including relevant user, endpoint, application and file activity.	Please refer to the relevant Addendum for updated specfications
961		Anti Phishing	19.23	Solution must have simplicity of evaluation and additional visibility into internal traffic and other communication channels can reduce risk, and baseline user activity to detect suspicious behavior.	Pre-Bid Query / Clarification: The existing clause already seeks baselining of user activity to detect suspicious behaviour. We request the Bank to clarify the intended depth and scope of this capability and whether enhanced monitoring may be applied to a focused population of up to 100 Bank-identified critical/high-risk users, where deeper visibility provides the greatest security value. Suggested Clarified Wording / Requested Action: Solution must provide additional visibility into relevant internal activity and communication channels to reduce risk and baseline user activity to detect suspicious behaviour. Enhanced user and data activity monitoring should be provided for up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, with configurable detection policies for suspicious, anomalous or policy-violating activities.	Please refer to the relevant Addendum for updated specfications
962		Anti Phishing	19.7	Solution must provide protection against harassment mail and mitigate the risks associated with emails from unknown senders specifically for executives or VIPs, safeguarding them from potential threats and ensuring their email communication remains secure.	Pre-Bid Query / Clarification: Since this clause already provides enhanced protection for executives/VIPs, we request the Bank to clarify whether such enhanced protection should extend beyond receipt of suspicious email to investigation of risky user and data activities that may occur following phishing or account compromise, for a limited set of the Bank's most critical users. Suggested Clarified Wording / Requested Action: Solution must provide protection against harassment mail and mitigate risks associated with emails from unknown senders specifically for executives or VIPs. For up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, the solution should additionally provide enhanced visibility into risky user and data activities following suspected phishing or account compromise, including relevant file movement, web/upload activity, removable-media activity and other supported data-transfer channels.	Please refer to the relevant Addendum for updated specfications
963		Cloud	1	OEM shall ensure compliance of the complete proposed solution & platform with RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and all applicable regulations throughout the contract period.	Pre-Bid Query / Clarification: We request the Bank to clarify that the OEM is required to maintain applicable security, privacy and regulatory controls relevant to the services provided and furnish available compliance/assurance documentation, while the overall regulatory compliance obligation of the Bank remains subject to the Bank's deployment, configuration and usage of the service. Suggested Clarified Wording / Requested Action: OEM shall maintain security, privacy and compliance controls applicable to the proposed hosted service and shall provide available independent assurance reports, certifications and relevant compliance documentation to support the Bank's obligations under applicable RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and other applicable regulatory requirements.	Please refer addendum for revised clause
964		Cloud	2	The Service uptime agreement for the proposed solution on cloud should have monthly uptime commitments and have transparent monthly credit calculations in case of uptime not being met for any services.	Pre-Bid Query / Clarification: We understand that published/contracted OEM hosted-service SLA commitments and corresponding service-credit methodology shall meet this requirement. Kindly confirm. Suggested Clarified Wording / Requested Action: Retain clause, with clarification that the applicable OEM hosted-service SLA and service-credit schedule will govern the commitment.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
965		Cloud	3	Solution provider should provide the design and process for data deletion in the scope of an independent audit and that the operational effectiveness of these controls is tested. The report for the same should be submitted to bank as and when asked by bank.	Pre-Bid Query / Clarification: For a globally operated hosted security service, control effectiveness is generally evidenced through independent assurance reports such as SOC 2 Type II and documented data-retention/deletion controls. We request the Bank to permit such independent assurance documentation instead of requiring a separate bespoke data-deletion audit report. Suggested Clarified Wording / Requested Action: Solution provider shall maintain documented secure data-retention and deletion controls. Compliance may be demonstrated through applicable independent third-party assurance reports/certifications (such as SOC 2 Type II or equivalent) and documented data-retention/deletion policies made available subject to OEM confidentiality requirements.	Please refer addendum for the revised clause
966		Cloud	4	Independent audit for testing effectiveness of secure data removal, such that data is rendered permanently inaccessible. (Including any backup or distributed online media).	Pre-Bid Query / Clarification: We request the Bank to accept independently audited secure deletion and media-management controls, together with documented retention/deletion periods, rather than requiring a customer-specific audit of all backup and distributed media. Suggested Clarified Wording / Requested Action: The OEM shall maintain secure data deletion, media handling and backup-retention controls designed to render customer data inaccessible in accordance with documented retention schedules. Effectiveness may be evidenced through independent assurance reports such as SOC 2 Type II/ISO 27001 or equivalent and relevant OEM security/privacy documentation.	Please refer addendum for the revised clause
967		Cloud	5	Bank shall have an option to implement 'Bring Your Own Key' as and when required.	Pre-Bid Query / Clarification: The proposed service protects data at rest and in transit using strong encryption; however, customer-managed infrastructure encryption keys are not a standard capability of the hosted anti phishing service. We request deletion of the BYOK requirement, or acceptance of OEM-managed enterprise-grade encryption and key-management controls. Suggested Clarified Wording / Requested Action: Requested Action: Delete the BYOK requirement. Alternatively: 'Data processed/stored by the hosted service shall be protected using industry-standard encryption in transit and at rest, with secure OEM-managed key-management controls subject to independent security assurance.'	Please refer addendum for the revised clause
968		Cloud	6	Web Application Firewall shall be implemented on the cloud for Web based applications. WAF application signature should be updated and reviewed regularly. The Report shall be submitted to bank on a periodic interval.	Pre-Bid Query / Clarification: Since the proposed platform is an OEM-managed hosted security service, underlying WAF technology, signatures and configurations form part of the OEM's internal security architecture and may not be exposed as customer-specific reports. We request the Bank to accept periodic VAPT/penetration-test assurance or equivalent independent security assessment evidence covering the hosted application instead of WAF signature reports. Suggested Clarified Wording / Requested Action: The hosted web application/platform shall be protected through appropriate application-security controls. The OEM shall conduct periodic vulnerability assessment and penetration testing/security assessments and, subject to confidentiality restrictions, provide an executive summary/attestation or applicable independent assurance evidence to the Bank on request. Customer-specific WAF signature reports shall not be mandatory.	Please refer addendum for revised clause
969		Cloud	7	The systems in cloud infrastructure should be periodically updated with the latest anti-malware signatures, the bidder shall submit the periodic report on the same with bank.	Pre-Bid Query / Clarification: For an OEM-managed hosted security service, infrastructure anti-malware/endpoint controls are centrally managed and independently audited. We request the Bank to accept OEM security assurance and vulnerability/malware-control attestations rather than periodic host-level signature reports. Suggested Clarified Wording / Requested Action: The OEM shall maintain appropriate malware protection, vulnerability management, patching and security monitoring controls for the hosted infrastructure. Compliance may be evidenced through independent assurance reports/certifications and applicable security-control attestations instead of customer-specific anti-malware signature update reports.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
970		Cloud	8	Data Loss Governance and risk management framework shall be defined by bidder for workload on the cloud and same shall be shared with bank on periodic basis. Data loss prevention controls should be implemented to secure the data in the cloud environment from unauthorized or inadvertent exfiltration.	Pre-Bid Query / Clarification: We request clarification that the requirement is intended to ensure protection against unauthorized/inadvertent data exfiltration through the proposed service and appropriate security controls for hosted customer data, rather than requiring disclosure of the OEM's internal cloud governance framework. Suggested Clarified Wording / Requested Action: The proposed solution shall provide configurable controls to identify and prevent unauthorized or inadvertent transmission/exfiltration of sensitive information through any channels. The OEM shall maintain appropriate access control, encryption and data-protection controls for customer data processed within the hosted service and provide applicable assurance documentation on request.	Please refer addendum for revised clause
971		Cloud	9	Log generation, storage and review process should be certified by CERT IN empaneled auditor, report for the same shall be submitted by bidder as and when required by bank.	Pre-Bid Query / Clarification: For global SaaS/POD services, security logging and monitoring controls are typically independently audited under recognized assurance frameworks. We request the Bank to accept SOC 2 Type II/ISO 27001 or equivalent independent assurance in lieu of a mandatory CERT-In-empanelled audit of the OEM's internal log-generation/storage/review process. Suggested Clarified Wording / Requested Action: The OEM shall maintain documented security logging, monitoring, retention and review controls. Effectiveness shall be evidenced through applicable independent third-party assurance reports/certifications such as SOC 2 Type II, ISO 27001 or equivalent. CERT-In-empanelled audit may be required only for bidder-managed components deployed specifically within the Bank environment, where applicable.	Please refer addendum for the revised clause
972		Cloud	10	IT Act 2000 & its amendments, and other Acts/Regulatory guidelines.	Pre-Bid Query / Clarification: Kindly clarify that the OEM must comply with legal/regulatory requirements applicable to it as the provider of the proposed hosted service and provide reasonable documentation to support the Bank's compliance obligations. Suggested Clarified Wording / Requested Action: OEM shall comply with applicable legal and regulatory obligations relevant to its provision of the proposed service and shall provide available security/privacy/compliance documentation reasonably required to support the Bank's applicable obligations.	Please refer addendum for the revised clause
973		Cloud	11	CERT IN Empaneled auditor report's is required for the following:	Pre-Bid Query / Clarification: We request the Bank to permit internationally recognized independent assurance reports/certifications for OEM-managed hosted services. CERT-In empanelled audit reports may remain applicable to India-specific bidder-managed/on-premises components where such audit is feasible and required. Suggested Clarified Wording / Requested Action: For OEM-managed hosted/SaaS services, independent assurance reports/certifications such as SOC 2 Type II, ISO 27001 or equivalent shall be accepted. CERT-In empanelled audit reports shall be applicable only to components/services for which such India-specific audit is contractually and technically feasible.	Please refer addendum for the revised clause
974		Cloud	12	The application and DB is/will be hosted separately on a dedicated infrastructure (physical/logical) for PSB. Evidence of dedicated infrastructure (physical/logical) for PSB should be submitted.	Pre-Bid Query / Clarification: The proposed platform is an OEM-managed hosted security service designed with logical access controls and customer data isolation. Requiring dedicated physical application/database infrastructure would restrict standard SaaS/POD architectures without necessarily improving the security outcome. We request acceptance of secure logical tenant/customer isolation supported by independent assurance evidence. Suggested Clarified Wording / Requested Action: The proposed hosted service shall provide secure logical segregation/isolation of Bank data and administrative access from other customers through appropriate access-control and tenant-isolation mechanisms. Dedicated physical application/database infrastructure shall not be mandatory where equivalent logical isolation is implemented and independently assured.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
975		Cloud	13	Feasibility to audit/review IT controls of the third party or obtaining independent review report for the same from CERT-In empaneled security consultant, to ensure it meets Bank's information security requirement.	Pre-Bid Query / Clarification: We request that the Bank permit review of current independent assurance reports/certifications as the primary mechanism for reviewing OEM IT controls. Any direct audit should remain subject to the OEM's standard contractual audit provisions, confidentiality, security, scope and advance-notice requirements. Suggested Clarified Wording / Requested Action: The Bank may review applicable independent third-party assurance reports/certifications covering the hosted service. Where additional audit is required, such audit shall be subject to mutually agreed scope, confidentiality/security restrictions, reasonable advance notice and the OEM's standard contractual audit provisions. A CERT-In empanelled consultant may review evidence made available under these conditions.	Please refer addendum for revised clause
976	29, 35 & 259	Sections 7.2.1, 7.2.4.1(b) & 16.21.2		Deception deployment and high-availability topology Section 7.2.1 (Deception Technology): "Any agent/Enforcer/Deceptor Standalone at DC and HA, N+N, Standalone at DR." Section 7.2.4.1(b): "The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active configuration." Section 16.21.2 (Decoy): "All the inline components of the solution must operate in high availability mode. In the event of any component failure, the system should automatically initiate failovers within seconds, ensuring uninterrupted functionality without requiring manual intervention."	The RFP describes the Bank-side deception components as standalone in Section 7.2.1, point no.- 4, but it is also mentioned HA and N+N. We request the bank to kindly clarify that in case we're deploying the solution on-prem, whether Bank needs the solution in Standalone mode/HA mode/N+N mode. Section 16.21.2 (Decoy), point no.-8, Bank has asked that all the inline components of solution should be in HA mode with automatic failover capability. However, the deception solution is not inline. Hence, we request Bank to clarify if they need the Deception Solution in HA. We request the Bank to add on-prem solution also in addition to Cloud/SAAS+Hybrid.	Please refer addendum for revised clause
977	68	Section 7.7 - On-cloud proposed solution OEM Responsibilities, Point 10	"The OEM shall have valid ISO/IEC 27001 certification and SOC 2 Type II report."	Cloud OEM certification requirement	We request the bank to accept ISO/IEC 27001 or SOC 2 Type II or both.	No Change, Please be guided by the RFP
978	29, 32 & 35	Sections 7.2.1, 7.2.3 and 7.2.4.1(b)		Responsibility for providing the Cloud/SaaS environment Section 7.2.1 (Deception Technology): "Cloud (SaaS) + Hybrid" Section 7.2.3: "The solution shall be hosted through a Cloud Service Provider (CSP), either fully as a SaaS service or through a combination of CSP-hosted and Bank-hosted components." Section 7.2.4.1(b): "Deception Technology: The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active configuration. The Cloud/SaaS deployment shall be aligned with the applicable SLA, RTO and RPO requirements."	7.2.4.1(b) We request the bank to kindly add the on-prem implementation option also for the core component of the Deception Solution.	Please refer addendum for revised clause
979	35 & 91	Sections 7.2.4.1(b) and 7.18.1 - Compute Infrastructure, Point 1		Hardware and VM infrastructure for Bank-hosted deception components Section 7.2.4.1(b): "Deception Technology: The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active configuration. The Cloud/SaaS deployment shall be aligned with the applicable SLA, RTO and RPO requirements." Section 7.18.1(1): "Bidders must design, size, supply, implement, maintain and manage suitable compute infrastructure for all the in-scope applications/solutions proposed in the RFP response."	We request the bank to kindly add the on-prem implementation option also for the core component of the Deception Solution.	Please refer addendum for revised clause
980	29-31	7.2 Solution & Services Deployment Model and Their HA Requirement	7.2.1 Solutions - Master Deployment Matrix (Sr. 7 Threat Intelligence Platform, Sr. 14 CTEM)	Deployment Mode 'Cloud (SaaS) + Hybrid'. Bank Location: Broker/Collector/Integrator - HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Management Console: Deployed at both Primary and Secondary sites.	For the TIP and CTEM solutions proposed as OEM-owned multi-tenant SaaS, a Bank-hosted broker/collector/integrator, agent, connector or separately installed management console may not be required depending on the OEM architecture. Bank is requested to confirm that, where the proposed OEM architecture does not require a Bank-hosted component, (a) the N+N Active-Active DC/DR requirement and (b) deployment of the management console at both Primary and Secondary sites are not applicable, and that the OEM's documented cloud-native HA/resiliency architecture meeting the applicable SLA, RTO and RPO requirements will be accepted as compliant.	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
981	31-33	7.2 Solution & Services Deployment Model and Their HA Requirement	Note below 7.2.1 and 7.2.3 Deployment Model Definition	'Partial HA deployment of any critical Bank-hosted component for which HA is mandated shall not be accepted.'	Bank is requested to confirm that this condition applies only to those components that the proposed OEM architecture actually requires to be hosted within the Bank's DC/DR, and that a pure-SaaS solution with no Bank-hosted component is not treated as 'partial HA'.	The HA requirement shall apply wherever HA is specified/mandated under the RFP for an on-premise/Bank-hosted component. Fully On-Premise: HA shall be implemented for all the solutions/components for which HA is mandated under the RFP as per the deployment requirement mandated in the RFP. Fully Cloud/SaaS: The cloud/SaaS service shall comply with the applicable availability, resilience and SLA requirements of the RFP. Hybrid- Component On-Premise and Cloud: HA, as per deployment requirement, shall be implemented for all components hosted within the Bank's DC/DR for which HA is mandated under the RFP. Cloud/SaaS components shall comply with the applicable cloud service availability, resilience and SLA requirements. Partial HA deployment shall not be accepted for any Bank-hosted component for which HA is mandated under the RFP.
982	259	16.21 Annexure 21: Sizing/Volumetrics, Data Retention and Current Infrastructure	16.21.2 Volumetrics - Solution-wise Requirements, Sr. 9 Threat Intelligence Platform	At least 5 user licenses. All the inline components of the solution must operate in high availability mode... automatically initiate failovers within seconds... Each node/environment must be individually provisioned for full peak load.'	Where the TIP is delivered as OEM-owned SaaS, node- or component-level provisioning may not be exposed to the customer. Bank is requested to confirm that platform-level HA, published architecture documentation and the contracted uptime SLA constitute compliance with the HA/failover intent of this volumetric requirement, and that node-level full-peak-load provisioning evidence is not required where those nodes are not customer-dedicated or customer-visible.	Please refer the addendum for revised clause
983	54 & 256-261	7.4 Functional Requirement - Services (Offsite Services) / Annexure 21	7.4 (f) read with 16.21.2 Volumetrics	Clause 7.4(f): 'The frequency and scope of each service shall be as specified in Annexure 21 - Sizing/Volumetrics.' Annexure 21, Clause 16.21.2 provides volumetrics only for the 14 Solutions; no volumetrics are stated for any of the nine Offsite Services.	No sizing parameters have been published for the nine Offsite Services, and these services cannot be scoped, licensed or priced on a comparable basis without them. Bank is requested to publish service-wise volumetrics, at minimum: (i) ASM - number of root domains, sub-domains, public IP ranges/ASNs, cloud accounts and related entities (overseas branches, subsidiaries, third parties); (ii) Dark Web Monitoring - number of monitored brands/keywords, executives/VIPs, domains, BIN ranges and customer records in scope; (iii) Anti-Phishing and Brand Protection - number of brands, logos, mobile apps, social media handles and the expected annual takedown volume; (iv) Threat Intelligence Feed - number of portal users, API call volume and IOC ingestion volume; (v) Phishing Simulation - number of users, campaigns per year and vishing/smishing volumes; (vi) Threat Hunting - data sources, log volume and hunt frequency; (vii) BAS and CART - number of assets/agents, scenarios and frequency.	No Change, Please be guided by the RFP.
984	258	16.21 Annexure 21	16.21.2 Volumetrics - Solution-wise Requirements	The S.No. column runs 1 (SIEM), then 4 (SOAR), 5 (XDR), 6 (NDR), 7 (UEBA)... S.No. 2 and 3 are absent.	We request you to please confirm that no solution volumetrics have been inadvertently omitted from Clause 16.21.2, and to re-issue the table with corrected serial numbering.	Please refer addendum for the revised clause
985	53-54	7.3.14 Continuous Threat Exposure Management (CTEM) Tool	7.3.14 read with Appendix 1A - Sheet 'Continous Threat Exposure Management (CTEM)' (69 line items / 690 marks)	Clause 7.3.14 defines CTEM as an integrated Vulnerability Management + Breach and Attack Simulation programme with a unified Risk Dashboard operationalising the five CTEM stages and attack-path visualisation. The Appendix 1A CTEM compliance sheet is predominantly an external digital-risk / threat-exposure specification (multilingual intelligence collection, compromised credential and payment-card detection, VIP/high-risk identity investigation reports, threat-actor interaction via dark web avatars, agentless continuous discovery of the digital footprint, reporting of malicious assets to external platforms and authorities).	The scope of CTEM in the RFP body and in the Appendix 1A compliance sheet are materially different technology categories. We request you to please to clarify which document governs, and to confirm whether CTEM is intended as (a) an internal VM + BAS correlation and validation platform, (b) an external CTEM / Digital Risk Protection platform, or (c) both. If both, We request you to please confirm whether a single OEM must provide the complete scope or whether the requirement may be met by an integrated combination of OEM platforms, and to split the Appendix 1A CTEM sheet accordingly.	The requirement is to have an integrated CTEM capability that integrates with and leverages relevant technologies such as VA/VM, BAS, ASM/EASM and other security controls/sources to provide a unified exposure view, risk-based prioritization, validation, attack-path analysis and remediation/mitigation workflows.
986	Appendix 1A	Appendix 1A - Functional Compliance Sheet (Solutions)	Sheet: Continous Threat Exposure Management (CTEM), S.No. 38 read with Clause 7.2.1 Sr. 14	S.No. 38: 'The solution should be deployed agentlessly, without requiring sensors or agents on endpoints, servers, or network appliances.' Clause 7.2.1 Sr. 14 requires CTEM as 'Cloud (SaaS) + Hybrid' with N+N Active-Active Bank-hosted components at DC and DR.	An agentless, sensor-less architecture is inconsistent with the Bank-hosted N+N Active-Active component requirement in the Master Deployment Matrix. We request you to please to reconcile the two and confirm that a fully agentless SaaS CTEM with no Bank-hosted component is acceptable and shall be scored as compliant.	Please refer addendum for revised clause
987	Appendix 1A	Appendix 1A - Functional Compliance Sheet (Solutions)	Sheet: Continous Threat Exposure Management (CTEM), S.No. 47, 48, 50, 51, 62	S.No. 47 'cross-platform IoC enforcement across the security stack'; S.No. 48 'assess and harden network, endpoint, and operating system security controls'; S.No. 50 'custom protections tailored to the organization's environment'; S.No. 51 'apply virtual patching/compensating controls/exposure mitigation mechanism to the firewall and other security systems'; S.No. 62 'leverage compensating controls and layered defense strategies'.	Functions such as enforcement, hardening and virtual patching are ordinarily executed by the Bank's NGFW, WAF, XDR, SOAR and endpoint controls. We request you to please confirm that these CTEM requirements may be met through API-based integration/orchestration and hand-off to the relevant enforcing control, rather than requiring the CTEM platform itself to perform native enforcement.	Please refer the addendum for revised clause
988	Appendix 1A	Appendix 1A - Functional Compliance Sheet (Solutions)	Sheet: Continous Threat Exposure Management (CTEM), S.No. 24	The solution should provide pre-built bidirectional integrations with SIEM, SOAR, ticketing (Manage Engine), and threat intelligence platforms.'	The clause names a specific ITSM product. We request you to please confirm the actual ITSM/ticketing platform(s) in use and to restate the requirement in vendor-neutral terms (REST API / webhook based bidirectional integration with the Bank's ITSM), so that the requirement is not brand-specific.	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
989	Appendix 1C / 56	Appendix 1C - Functional Compliance Sheet (Services)	Sheet: Anti-Phishing Services (1,130 marks), S.No. 1 to 19.81, read with Clause 7.4.5	The majority of the Anti-Phishing sheet specifies a secure email gateway / email security platform: MTA forwarding to on-prem mail gateways, inbound/outbound policy rules and quarantine with release workflow, enforced TLS 1.2 for inbound and outbound mail, user/group synchronisation with on-prem AD and Azure AD, SAML 2.0, integration with On-Prem and Cloud Exchange, storing a copy of emails at first entry point, BEC/EAC blocking, Impostor classifier and composite spam scoring, directory harvest and DoS protection, and an 'Intel source which processes more than 3.4 Trillion Mails in a Year'. Clause 7.4.5 (Page 56) scopes Anti-Phishing solely as offsite monitoring and response for phishing websites, domains, URLs, brand/domain impersonation and fraudulent digital assets. No email security solution appears in Clause 7.2.1 Master Deployment Matrix, Annexure 19 Stack Confirmation Sheet (Page 250-251) or Appendix 2 Bill of Material.	We request you to please to clarify whether secure email gateway / email security capabilities are within the scope of this RFP. If they are not, please confirm that the related line items in the Anti-Phishing Services sheet will be treated as Not Applicable or reconsiderd through corrigendum, without adverse scoring. If such capabilities are in scope, please identify the corresponding solution/service line, deployment model, volumetrics and commercial/MAF requirements so that they can be quoted appropriately.	Please refer to the relevant Addendum for updated specfications
990	Appendix 1C / 57	Appendix 1C - Functional Compliance Sheet (Services)	Sheet: Threat Intelligence Feed (200 marks), S.No. 4, 7, 8, 9, 13, 14, 15, 16, 17, 20	Several line items prescribe implementation-specific feature names, report taxonomy and malware-analysis mechanics - including browser lookup, sandbox/file-detonation detail, retrospective hunting terminology, malware corpus access, YARA-oriented hunting, relationship-graph pivoting and named report constructs.	We request you to please to restate these items in OEM-neutral, outcome-based terms so that qualified threat-intelligence providers can respond on comparable functional outcomes. For example: retrospective hunting over historical intelligence; user-defined hunting/detection logic; contextual relationship analysis across indicators, actors, campaigns and malware; and periodic strategic, adversary, malware, vulnerability and sectoral intelligence reporting. Where malware sandboxing is required as a distinct capability, We request you to please to identify it separately in the solution stack/BOM.	No Change, Please be guided by the RFP.
991	Appendix 1C / 57	Appendix 1C - Functional Compliance Sheet (Services)	Sheet: Threat Intelligence Feed, S.No. 7, 9, 20 read with Clause 7.4.7	S.No. 7, 9 and 20 require malware sandbox detonation, malware file corpus download and multi-engine file scanning. Clause 7.4.7 (Page 57) scopes the Threat Intelligence Feed as IOC, IOA, threat actor and campaign intelligence, malware and ransomware intelligence, vulnerability and exploit intelligence, sectoral intelligence, MITRE ATT&CK mapping, enrichment and prioritisation.	A malware analysis / sandbox platform is a distinct technology category from a curated threat intelligence feed. We request you to please confirm whether a malware analysis and sandboxing platform is separately in scope and, if so, under which line of Annexure 19 (Stack Confirmation Sheet) and Appendix 2 (Bill of Material) it is to be declared and quoted.	No Change, Please be guided by the RFP. Such capabilities, where required, shall be provided as part of the offsite Threat Intelligence Feed service and shall not require separate on-premise infrastructure or licence procurement by the Bank.
992	Appendix 1C / 32, 250-251	Appendix 1C / Annexure 19 / Appendix 2	Sheets: Anti-Phishing Services, Brand abuse, Dark Web Monitoring, Threat Intelligence Feed	Look-alike and typo-squatted domain monitoring, fraudulent mobile application detection, social media and executive impersonation monitoring, phishing infrastructure detection and takedown are independently specified in the Dark Web Monitoring sheet (e.g. S.No. 13, 17, 18, 20, 33, 34, 41, 42, 52), the Brand abuse sheet and the Anti-Phishing Services sheet. Annexure 19 and Appendix 2 require a separate Make / Tool Proposed and a separate priced line for Anti-Phishing (AP), Dark Web Monitoring (DWM), Brand Protection & Monitoring (BPM) and Threat Intelligence Feed (TIF).	Where a single OEM platform delivers two or more of these services, the same capability and the same licensed data would otherwise be quoted and procured multiple times. We request you to please confirm that (a) one OEM platform may be declared against multiple service lines in Annexure 19, (b) the capability need not be licensed or priced more than once, and (c) how such consolidation will be normalised during commercial evaluation so that consolidated and multi-vendor bids are compared on a like-for-like basis.	Please refer to the relevant Addendum for updated specfications
993	Appendix 1C / 32, 58, 251	Appendix 1C / 7.2.2 / 7.4.9 / Annexure 19	Sheet names 'Brand abuse' and 'Attack Surafce Management'	The Appendix 1C sheet is titled 'Brand abuse', whereas Clause 7.2.2 (Page 32), Clause 7.4.9 (Page 58) and Annexure 19 (Page 251) refer to the service as 'Brand Protection and Monitoring'. The Attack Surface Management sheet is titled 'Attack Surafce Management'.	We request you to please confirm that 'Brand abuse' and 'Brand Protection and Monitoring' refer to the same service, and to issue corrected sheet names, so that the OEM declaration in Annexure 19 and the compliance sheet can be mapped unambiguously.	Brand Abuse here refers to Brand Protection and Monitoring
994	Appendix 1C	Appendix 1C - Functional Compliance Sheet (Services)	Sheet: Attack Surafce Management, S.No. 14	All the software modules of the proposed solution should be latest as well as stable one and must have a general release date prior to the date of the submission of the proposal.'	Attack Surface Management is required at Clause 7.2.2 to be delivered as a Managed Service on a continuously updated SaaS platform, which has no discrete module-level general release date. We request you to please to accept an OEM declaration that the service is delivered on the current generally available production release of the platform, in lieu of module release dates.	Please refer addendum for revised clause.
995	Appendix 1C	Appendix 1C - Functional Compliance Sheet (Services)	Sheet: Attack Surafce Management, S.No. 20 and 21	'The solution should automatically discover the bank's assets exposed to internet, including the assets of all the entities owned by and related to bank such as overseas branches, subsidiaries, third-parties, mergers, acquisitions etc.' and 'discover inventory of known and unknown assets of bank, metadata, shadow IT assets... discover new seeds which may lead to attack surface.'	We request you to please provide the number of related entities (overseas branches, subsidiaries, third parties, RRBs and any other affiliates) to be covered, as this directly determines service sizing and pricing. Bank is further requested to confirm that the Bank will furnish and formally authorise the initial seed list (domains, IP ranges, ASNs, brand names), since attribution and monitoring of third-party owned assets requires the Bank's written confirmation of ownership.	No Change, Please be guided by the RFP
996	Appendix 1C / 57-58	Appendix 1C / 7.4.8 Threat Hunting Services	Sheet: Threat Hunting Services, S.No. 15; Sheet: Anti-Phishing Services, S.No. 37	'Bidder should be able to identify and report to the bank if access to blocked ports on a webserver is sought by an external user.'	Detection of connection attempts to blocked ports requires the Bank's own firewall, WAF and web server telemetry and cannot be derived from external intelligence sources. We request you to please confirm that the Bank will provide the required log feeds, and that this line item is assessed against the SIEM / SOC service rather than against the offsite intelligence service OEM.	Please refer addendum for revised clause.
997	57-58	7.4.8 Threat Hunting Services	7.4.8 (f), (g), (m)	The service is defined as 'offsite, tool-based' yet requires 'Detection engineering and security use-case tuning', 'Correlation rule optimization' and delivery 'remotely/offsite using secure and mutually agreed mechanisms for accessing relevant logs, telemetry, security tools, and data made available by the Bank.'	We request you to please to specify the access model to be provided to the offsite threat hunting provider (read-only API/log export to the provider's platform, versus direct interactive access to the Bank's SIEM console), and to confirm that accountability for implementing and validating any correlation-rule change in the production SIEM remains with the SIEM OEM and the SI, with the threat hunting provider responsible for recommending the detection logic.	The threat-hunting provider shall remain responsible for the required analysis, detection engineering, use-case tuning, correlation-rule optimization and provision of recommended detection logic

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
998	Appendix 1A p.1-9 (PDF p.3-11)	Appendix 1A - Cloud Deployment Requirement (applies to all cloud-deployed solutions)	Sheet: 'All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution' - S.No. 1 to 67	The sheet is drafted for a Bank workload hosted by the Bidder on IaaS/PaaS - e.g. S.No. 32 VM image encryption, USB disabling on VMs, VMs on dedicated partitions and non-shared IP addresses; S.No. 45.1-45.6 network segregation by environment, landing segment for ingress, DMZ routing, micro-segmentation, firewall/IPS/anti-DDoS/AV/DLP/WAF/NAC on all segments; S.No. 49 WAF on the cloud; S.No. 50 Secure SDLC with security assurance certificate; S.No. 7 and 59 patching and tech refresh of provisioned infrastructure; S.No. 60 OS/DB/network device/VM/middleware hardening per Bank SCD. Clause 7.2.1 mandates 'Cloud (SaaS)' as the deployment mode for SIEM, SOAR, UEBA, Decoy, XDR, TIP, CSPM, CNAPP, CWPP and CTEM, and Clause 7.2.2 mandates 'Managed Service' for all nine Offsite Services.	Where a solution or service is delivered as OEM-owned multi-tenant SaaS, the Bank and the Bidder neither own nor operate the underlying infrastructure, and these controls are implemented and audited by the OEM within its own platform rather than configured for the Bank. We request you to please to either (a) issue a SaaS-specific variant of the Cloud Deployment Requirement sheet, or (b) confirm that for SaaS-delivered solutions and services, compliance against the infrastructure-level items may be evidenced through the OEM's ISO/IEC 27001 certificate, SOC 2 Type II report, independent penetration test summary, platform security whitepaper and shared-responsibility matrix, and shall be scored as compliant on that basis.	The bidder may submit available public/summary SBOM/CBOM information at bid stage, subject to the RFP. Detailed confidential information may be provided post-award under applicable confidentiality/security arrangements. However, the Bank reserves the right to require sufficient component, vulnerability and dependency information for security assurance. Machine-readable formats such as SPDX/CycloneDX may be accepted where they contain all required information as shall be required/highlighted by Cert IN /Regulator.
999	Appendix 1A p.1 / 67 / 68	Appendix 1A - Cloud Deployment Requirement	S.No. 1 read with Clause 7.6.8 item 6 and Clause 7.7.11	Cloud Deployment Requirement S.No. 1: 'Cloud must be hosted in India, and there should be no network and data sharing/replication to any datacenter/office outside the boundaries of India.' Clause 7.7.11: 'All Bank data, including production data, backups, logs, telemetry, prompts, metadata, and related information, shall reside within India. No data shall be transmitted, processed, stored, validated, replicated, or accessed outside India without prior written approval from the Bank and applicable regulatory authorities.'	We request you to please to clarify how the India data-residency requirement applies to globally sourced external intelligence and third-party takedown coordination. Please confirm that (a) the Bank's tenant, Bank-specific findings, alerts, reports and configuration data at rest are to be hosted in India; (b) collection of external threat intelligence and coordination with registrars, hosting providers, app stores, browser vendors and social-media platforms outside India are permitted as part of the service; (c) any remote support or analyst access from outside India, where required, may be provided only under the Bank-approved access controls and audit requirements; and (d) the approval mechanism under Clause 7.7.11 may be agreed contractually rather than obtained transaction by transaction.	No Change, Please be guided by the RFP
1000	Appendix 1A p.1	Appendix 1A Cloud Deployment Requirement	S.No. 6	'Where the solution is hosted, CSP should be empaneled with the Ministry of Electronics and Information Technology (MeitY).'	SaaS OEMs typically host their India tenants on a hyperscaler's India region; the OEM itself is not a MeitY-empanelled CSP. We request you to please confirm that hosting the Bank's tenant within a MeitY-empanelled CSP's India region satisfies this requirement, and that the SaaS OEM is not itself required to be MeitY empanelled.	No Change, Please be guided by the RFP
1001	Appendix 1A p.1-2	Appendix 1A Cloud Deployment Requirement	S.No. 2, 3, 18	S.No. 2 provisioning of switches, routers, firewalls and load balancers with all devices in HA and no single point of failure; S.No. 3 cloud infrastructure deployed in HA (N+N) at both primary and secondary site; S.No. 18 cloud infrastructure presence in at least 2 cities in India in different seismic zones.	For SaaS, the network and infrastructure layer is owned and operated by the OEM/CSP and is not provisioned by the Bidder. We request you to please confirm that the OEM's documented cloud-native HA/resiliency architecture, meeting the applicable India hosting/data-residency requirements and the specified RTO, RPO and uptime requirements, is deemed compliant, and that S.No. 2, 3 and 18 apply only where the Bidder builds and controls the hosting topology.	No Change, Please be guided by the RFP
1002	Appendix 1A p.2-4	Appendix 1A Cloud Deployment Requirement	S.No. 11, 31.2, 31.3	S.No. 11: 'Bank will have right to audit the data center facilities of CSP through any regulators or through any third parties...' S.No. 31.2: 'Bank must have Rights to Audit the compliance with the CSP agreement including rights of access to the CSP's premises where relevant records and Bank's data is being held.'	Hyperscale cloud service providers typically do not grant individual customers or their auditors physical access to data-centre premises; assurance is provided through independent audit and compliance attestations. We request you to please confirm that the applicable CSP audit/compliance reports, together with the OEM's own audit cooperation, evidence submission and remediation commitments, satisfy S.No. 11 and 31.2, and that the OEM/Bidder will not be held in breach solely because the CSP's standard terms do not permit physical premises access.	No Change, Please be guided by the RFP
1003	Appendix 1A p.2	Appendix 1A Cloud Deployment Requirement	S.No. 12	'The Solution provider should provide bank, the third-party audit reports on information security & data integrity, source code review including APIs, details about APIs encryption of payloads, authorization, and authentication API wise - every year irrespective of any audit on demand.'	Source code of proprietary SaaS platforms is generally not made available to customers or customer auditors. We request you to please to accept, in lieu of source-code review, appropriate independent application-security / secure-SDLC assurance, an annual VAPT summary and API/security documentation covering authentication, authorisation and encryption controls, and to confirm that such evidence will be treated as compliant for a SaaS deployment.	No Change, Please be guided by the RFP
1004	Appendix 1A p.2-4 / 68	Appendix 1A - Cloud Deployment Requirement	S.No. 14, 27, 44 read with Clause 7.7.1 and 7.7.2	S.No. 14: 'Each of the environments provided should be logically isolated, i.e., separate from the production environment in a different VLAN than the production environment...'; S.No. 27: resource pooling / multi-tenancy with logical separation between each consumer's computing resources and network; S.No. 44: 'Bank's data should be isolated from other customers, to avoid comingling of data, in case of multi-tenancy.' Clause 7.7.1 and 7.7.2 require a dedicated tenant/workspace provisioned for the Bank.	We request you to please confirm that logical tenant isolation in a multi-tenant SaaS architecture - with a dedicated Bank tenant/workspace, per-tenant access control, tenant-scoped data segregation and encryption at rest - satisfies S.No. 14, 27, 44 and Clause 7.7.1-7.7.2, and that a physically dedicated instance, dedicated VLAN or single-tenant deployment is not mandated.	Please refer addendum for the revised clause
1005	Appendix 1A p.2	Appendix 1A Cloud Deployment Requirement	S.No. 23	'The proposed solution should also have Service level commitments for virus detection and blocking, spam effectiveness, false positives as well as email delivery.'	This item appears to relate to email security gateway controls and its applicability to the listed cloud/SaaS solutions and services is unclear. We request you to please to clarify the specific solution/service to which S.No. 23 applies, or to confirm that it may be marked Not Applicable without adverse scoring where the proposed solution does not provide email security gateway functionality.	Please refer addendum for revised clause
1006	Appendix 1A p.3	Appendix 1A Cloud Deployment Requirement	S.No. 24	'Perform regular backup and recovery tests at cloud primary and secondary sites as well as enable sharing the data, configurations rules and policies with the bank for backup at bank's premise.'	For OEM-owned SaaS, the platform's detection logic, collection rules and internal configuration are OEM intellectual property and cannot be exported to a customer's premises. We request you to please confirm that export of the Bank's own data - findings, alerts, incidents, reports, IOCs and tenant-level configuration - in machine-readable formats (REST API, CSV, JSON, STIX/TAXII) on a scheduled basis satisfies this requirement.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1007	Appendix 1A p.3-6	Appendix 1A Cloud Deployment Requirement	S.No. 31.4, 34, 63	S.No. 31.4 'Integration of all devices with Bank's SOC, SIEM & other security solution for monitoring'; S.No. 34 devices integrated with Bank's SOC for access, threat, audit and administrator log monitoring; S.No. 63 'All logs of assets related to Bank's subscription/tenant should be integrated with the Bank's SOC.'	For SaaS, infrastructure- and hypervisor-level logs of the OEM's shared platform cannot be exported to a customer SOC. We request you to please confirm that tenant-scoped audit logs - user authentication, administrative actions, configuration changes, data access, alerts and findings - delivered to the Bank's SIEM via API or syslog satisfy S.No. 31.4, 34 and 63.	Please refer addendum for revised clause
1008	Appendix 1A p.4-5	Appendix 1A Cloud Deployment Requirement	S.No. 32, 45.1 to 45.6, 46.5, 46.6, 49, 50, 52, 54, 60	Virtual environment security including VM image encryption, USB disabling on VMs and dedicated partitions (S.No. 32); network segregation by environment, landing segment, DMZ routing, micro-segmentation and full security-control stack on every segment (S.No. 45.1-45.5); direct network connection with cryptographic controls between cloud and on-premises (S.No. 45.6); prohibition of administrator remote access over the Internet (S.No. 46.5); WAF for web applications on the cloud (S.No. 49); Secure SDLC with security assurance certificate (S.No. 50); anti-malware signature updates (S.No. 52); file integrity monitoring (S.No. 54); secure configuration per Bank SCD for OS/DB/network devices/VMs/middleware (S.No. 60).	These are infrastructure controls internal to the OEM's SaaS platform and are generally neither configurable by the Bank nor separately evidenceable per customer tenant. We request you to please to mark these items as applicable to Bidder-managed cloud (IaaS/PaaS) deployments only, or to accept for SaaS the OEM's applicable certifications, penetration-test summary and security documentation as evidence. Where the SaaS administration interface is remotely accessible, appropriate controls such as MFA, RBAC, IP allow-listing where supported, and full audit logging should be accepted as the relevant control evidence.	Please refer addendum for the revised clause
1009	Appendix 1A p.5 / 32 / 54	Appendix 1A - Cloud Deployment Requirement	S.No. 46.7 read with Clause 7.2.2 and Clause 7.4(d)	S.No. 46.7: 'Solution provider /Cloud Service Provider/ Cloud Management Team should not have access to any application data of the Bank.'	Where an Offsite Managed Service requires OEM analysts to access the OEM-hosted Bank tenant/workspace or tenant-scoped findings/configuration to deliver the contracted service, We request you to please to reconcile S.No. 46.7 with Clauses 7.2.2 and 7.4(d), and to confirm that such access is permitted under least-privilege RBAC, approved privileged-access controls and full audit logging. This clarification should not be construed as requiring direct OEM access to the Bank's internal systems unless such access is separately specified and approved.	No Change, Please be guided by the RFP
1010	Appendix 1A p.5 / 68	Appendix 1A - Cloud Deployment Requirement	S.No. 47.2, 47.3, 47.5 read with Clause 7.7.4	S.No. 47.2: 'Bank shall have an option to implement Bring Your Own Key as and when required'; S.No. 47.3: in case cloud based HSM is used it should meet FIPS 140-2 Level 3 and above; S.No. 47.5: where CSP/Solution provider keys are used for encryption of Bank's data, such keys should be unique and not shared by other users of the cloud service. Clause 7.7.4: 'The proposed Cloud/SaaS solution shall support Bring Your Own Key (BYOK) and/or Customer-Managed Encryption Key (CMEK) capability, enabling the Bank to maintain control over the cryptographic keys used to protect its security data.'	Multi-tenant cyber-intelligence SaaS platforms commonly encrypt tenant data at rest using CSP-managed or OEM-managed key-management services and may not expose BYOK/CMEK to individual tenants. We request you to please confirm whether BYOK/CMEK is a mandatory requirement for every cloud solution and service, or whether strong encryption at rest with documented OEM/CSP key management, rotation and logical tenant isolation is acceptable where BYOK/CMEK is not supported by the OEM architecture. Clarity is required at pre-bid stage as this materially affects OEM selection.	Please refer addendum for revised clause
1011	68	7.7 On-cloud proposed solution OEM Responsibilities	7.7.6 and 7.7.7	7.7.6: 'The bidder/OEM shall establish and manage a dedicated cloud landing zone, including Development, UAT, and Production environments, with appropriate segregation, governance, access controls, monitoring, and SDLC controls.' 7.7.7: responsibility for provisioning, configuration, administration, monitoring, patching, upgrading, backup, recovery, migration and lifecycle management of all cloud resources including compute, storage, databases, containers and networking.	For a subscription SaaS solution or Managed Service there is no Bank-dedicated cloud landing zone and no Bank-dedicated Development/UAT/Production estate; the OEM operates a single continuously-maintained platform with logically isolated customer tenants. We request you to please confirm that Clause 7.7.6 and 7.7.7 apply only to cloud environments built and operated by the Bidder on the Bank's behalf, and that for SaaS the OEM's provision of a production tenant (and a sandbox/UAT tenant where the OEM offers one) with documented change management satisfies the requirement.	No Change, Please be guided by the RFP
1012	Appendix 1A p.3-4	Appendix 1A Cloud Deployment Requirement	S.No. 28, 29, 30, 38, 41.1 to 41.5	Secure data deletion with no data remanence; independent audit of the data deletion design and its operational effectiveness; confirmation that Bank data is rendered permanently inaccessible including in backups; reverse data shifting on contract completion or termination; and a documented exit plan.	We request you to please confirm the acceptable evidence format, namely (a) an OEM-issued certificate of data deletion referencing its documented deletion procedure and retention/backup expiry cycle, (b) export of Bank data via API in open formats prior to deletion, and (c) evidence of independent testing of deletion controls through the OEM's existing SOC 2 Type II or ISO/IEC 27001 audit scope, rather than a separate Bank-commissioned audit of the OEM's platform.	Please refer addendum for the revised clause
1013	68	7.7 On-cloud proposed solution OEM Responsibilities	7.7.10	The OEM shall have valid ISO/IEC 27001 certification and SOC 2 Type II report.'	We request you to please confirm (a) whether the ISO/IEC 27001 certificate and SOC 2 Type II report are to be submitted with the technical bid or may be furnished post-award under a confidentiality undertaking (SOC 2 Type II reports are ordinarily released only under NDA), and (b) whether additional/alternative certifications such as ISO/IEC 27017, ISO/IEC 27018 or ISO/IEC 27701 will be recognised.	Please refer addendum for the revised clause
1014	59 / 249 / 253-255	7.6 OEM Responsibilities / Annexure 18 / Annexure 20	Clause 7.6.9, Annexure 18 clause 5, Annexure 20 (a) S-BOM and (b) C-BOM	Annexure 20 requires, for every component of every proposed tool/solution, the Version, Description, Supplier, Licence, Origin, Dependencies, Vulnerabilities, Patch Status, Release Date, End of Life Date, Usage Restrictions, Checksums, Hashes, Executable Property, Archive Property, Structured Property and Unique Identifier, on OEM letterhead. Annexure 18 clause 5 provides that the SBOM and 'CBOM - Public' are attached at bid stage and that 'the detailed/private SBOM and CBOM containing confidential or sensitive security information shall be provided to the Bank after issuance of the Purchase Order and execution of applicable confidentiality requirements.'	For OEM-owned multi-tenant SaaS, a detailed component inventory including dependency, vulnerability, patch-status and hash information is often treated as sensitive security information and may not be released at bid stage. We request you to please confirm, consistent with Annexure 18 clause 5, that SaaS OEMs may submit at bid stage (a) an available summary/public SBOM and CBOM in an industry-standard machine-readable format such as CycloneDX or SPDX and (b) an undertaking to provide any additional detailed disclosure required post-award through an agreed controlled/NDA process. Please also confirm that the Annexure 20 tabular layout is indicative and that an accepted machine-readable BOM format may be submitted in its place.	The bidder may submit available public/summary SBOM/CBOM information at bid stage, subject to the RFP. Detailed confidential information may be provided post-award under applicable confidentiality/security arrangements. However, the Bank reserves the right to require sufficient component, vulnerability and dependency information for security assurance. Machine-readable formats such as SPDX/CycloneDX may be accepted where they contain all required information as shall be required/highlighted by Cert IN /Regulator.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1015	59	7.6 OEM Responsibilities	7.6.9	'The OEM shall maintain and periodically (Quarterly or as required by regulators) update Software Bill of Materials (SBOM), Cryptographic Bill of Materials (CBOM), Quantum Bill of Materials (QBOM), AI Bill of Materials (AI-BOM), and all dependent components in accordance with applicable CERT-In guidelines and regulatory requirements.'	The RFP requests QBOM and AI-BOM information but does not identify the required schema or minimum data elements. We request you to please to specify the expected standard and content for these submissions. Please also confirm whether CycloneDX CBOM for cryptographic-asset inventory and CycloneDX ML-BOM for AI/ML model and dataset inventory are acceptable for the corresponding requirements, and clarify any additional information expected specifically under the term 'QBOM'.	The OEM shall maintain and periodically update the applicable SBOM, CBOM, AI-BOM and QBOM information in accordance with applicable CERT-In guidelines, regulatory requirements and prevailing industry standards. The relevant BOM information shall, as applicable, include identification of the component/asset, version, supplier/OEM, dependencies, relationships, vulnerabilities/security advisories, licensing information and relevant security attributes. Where a specific regulatory authority or applicable standard subsequently prescribes a particular schema, format or additional data elements, the OEM shall comply with the same during the contract period, subject to the applicable regulatory requirements. The bank will specify the BOM format/schema proposed, data elements captured, frequency of update, scope of coverage and mechanism inline with the requirement prescribed by regulator/statutory bodies.
1016	253-255	16.20 Annexure 20: S-BOM & C-BOM Details	Annexure 20, rows 'Version', 'Release Date', 'End of Life Date'	The template requires a Version, Release Date and End of Life Date for each component.	For a continuously updated SaaS platform, component-level Version, Release Date and End-of-Life fields do not map cleanly to customer-selectable releases. We request you to please confirm that a service-level declaration such as 'SaaS - continuously updated; current generally available production service', together with an undertaking to maintain a supported service throughout the contract period and notify the Bank of material lifecycle changes, is acceptable for SaaS-delivered solutions and services in Annexure 20, Annexure 18 and Annexure 8.	For SaaS-delivered solutions/services where the solution is continuously updated by the OEM and customer-selectable component-level releases, release dates and end-of-life dates are not applicable. However, OEM shall confirm the below in their undertaking SaaS service shall remain supported, maintained and available throughout the contract period, in accordance with the RFP/SLA requirements, and shall notify the Bank in advance of any material lifecycle changes, service discontinuation, major architecture changes or planned end-of-support/end-of-service events that may affect the Bank.
1017	26	7.1 Scope and Objectives	7.1, paragraph on PQC readiness	The proposed solution shall support PQC readiness, including support for secure cryptographic mechanisms and standards that facilitate future migration to quantum-resistant cryptography, wherever applicable to the solution.'	We request you to please to specify the evidence expected to demonstrate PQC readiness at bid stage (for example, disclosure of cryptographic primitives in the CBOM together with a published OEM PQC migration roadmap), the NIST PQC algorithms in scope (ML-KEM, ML-DSA, SLH-DSA), and the timeline within the contract period by which PQC algorithm support must be delivered, so that this can be committed and priced consistently.	The OEM shall maintain and periodically update the applicable SBOM, CBOM, AI-BOM and QBOM information in accordance with applicable CERT-In guidelines, regulatory requirements and prevailing industry standards. The relevant BOM information shall, as applicable, include identification of the component/asset, version, supplier/OEM, dependencies, relationships, vulnerabilities/security advisories, licensing information and relevant security attributes. Where a specific regulatory authority or applicable standard subsequently prescribes a particular schema, format or additional data elements, the OEM shall comply with the same during the contract period, subject to the applicable regulatory requirements. The bank will specify the BOM format/schema proposed, data elements captured, frequency of update, scope of coverage and mechanism inline with the requirement prescribed by regulator/statutory bodies.
1018	222 / 248 / 250-252	Annexure 8 / Annexure 18 / Annexure 19	Annexure 8 clause 3 and table 'Product Version / Edition'; Annexure 18 clause 3; Annexure 19 'Model of the Product'	Annexure 8 clause 3: 'We confirm that the product/version proposed under this RFP is the latest available production version as on the date of submission of the Bid.' Annexure 18 clause 3: 'the OEM make, model, and version declared herein are identical to those proposed by the bidder...' Annexure 19 clause 4 provides that any discrepancy or substitution of OEM/model may render the bid liable for rejection.	Subscription SaaS platforms and Managed Services are continuously updated and do not carry a customer-selectable model or version. We request you to please to permit SaaS OEMs to declare 'SaaS - continuously updated; current generally available production release' in the Model / Version / Edition fields of Annexure 8, Annexure 18 and Annexure 19, and to confirm that such a declaration, and subsequent routine platform updates during the contract, shall not be construed as a discrepancy or substitution under Annexure 19 clause 4.	The OEM shall maintain and periodically update the applicable SBOM, CBOM, AI-BOM and QBOM information in accordance with applicable CERT-In guidelines, regulatory requirements and prevailing industry standards. The relevant BOM information shall, as applicable, include identification of the component/asset, version, supplier/OEM, dependencies, relationships, vulnerabilities/security advisories, licensing information and relevant security attributes. Where a specific regulatory authority or applicable standard subsequently prescribes a particular schema, format or additional data elements, the OEM shall comply with the same during the contract period, subject to the applicable regulatory requirements. The bank will specify the BOM format/schema proposed, data elements captured, frequency of update, scope of coverage and mechanism inline with the requirement prescribed by regulator/statutory bodies.
1019	221 / 27 / 59-63	Annexure 8 / 7.1 / 7.6	Annexure 8 clause 1(a) read with Clause 7.1(a)(a), 7.6.1 to 7.6.6	Annexure 8 clause 1(a): 'Scope of work pertaining to Requirement Analysis, System Design, Development & Implementation, Documentation, Final Deployment and Go-Live for our proposed product/solution shall be performed by us as specified in the RFP.' Clause 7.6.2 and 7.6.4 require the OEM to prepare and submit HLD, LLD, deployment architecture, integration architecture, configuration guides, SOPs, operational manuals and as-built documentation, and Clause 7.6.1 requires a Functional Requirement Specification Manual.	For subscription SaaS solutions and Managed Services there is typically no customer-specific software development or Bank-managed infrastructure build unless explicitly scoped. OEM delivery generally consists of tenant provisioning, onboarding and scoping, configuration of use cases, integration enablement, UAT support, go-live and knowledge transfer. We request you to please confirm that, for SaaS-delivered solutions and services, the OEM's obligation under Annexure 8 clause 1(a) and Clause 7.6 may be discharged through a Solution Architecture / Service Design document, integration and data-flow design, configuration/onboarding record, SOPs/runbooks, UAT support and an OEM Go-Live certificate, in place of infrastructure HLD/LLD/as-built documentation that is not applicable to the SaaS architecture.	Bidder to design and provide all relevant document For SaaS-delivered solutions, infrastructure-specific HLD/LLD or as-built documentation that is not applicable to the proposed SaaS architecture may be replaced with equivalent solution-specific documentation covering solution architecture/service design, integration architecture and data flows, configuration/onboarding details, applicable SOPs/runbooks, operational and administration procedures, UAT support and Go-Live documentation/certificate

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1020	222	Annexure 8: Certification on OEM Requirements	Annexure 8 clause 1(e)	The OEM shall provide the Bank with advance written notice of any material change, update, discontinuation, End-of-Sale (EoS), End-of-Life (EoL) or End-of-Support (EoS) event that may impact the Services. For any event likely to cause service disruption or discontinuity or materially impact the Services/SLAs, the OEM shall provide a minimum of six (6) months' prior written notice, wherever practicable, and support continuity/transition requirements.	We request you to please confirm that the six-month advance-notice requirement, stated to apply 'wherever practicable' to events likely to cause service disruption/discontinuity or materially affect Services/SLAs, does not extend to routine SaaS feature releases, UI changes, security patches or normal platform maintenance that do not materially degrade a contracted capability or SLA; such routine changes would follow the OEM's standard release-note/maintenance-notification process.	The requirement for six (6) months' advance written notice is intended for material events such as discontinuation, End-of-Sale (EoS), End-of-Life (EoL), End-of-Support, or other changes likely to cause service disruption/discontinuity or materially impact the contracted Services, functionality or SLAs. The six-month advance-notice requirement shall not apply to routine SaaS lifecycle activities, including normal feature releases, UI/UX changes, security patches, bug fixes, minor enhancements, routine updates/upgrades and scheduled platform maintenance, provided that such changes do not degrade or discontinue any contracted functionality, security capability, service availability or SLA commitment.
1021	224	Annexure 8: Certification on OEM Requirements	Annexure 8 clause 9	'For all incidents related to the supplied solution, the OEM shall provide the Bidder/Bank with an OEM-issued RCA report within three (3) working days from the date of incident resolution...'	We request you to please confirm that the OEM RCA obligation applies to incidents attributable to the OEM's platform or service (availability, product defect or security incident); that the three working day timeline applies to Severity 1 and Severity 2 incidents with a mutually agreed timeline for lower severities; and that incidents arising from the Bank's infrastructure, third-party integrations, data source availability or the System Integrator's configuration are outside the OEM RCA obligation.	The OEM shall provide an OEM-issued RCA report for incidents attributable to the supplied solution/OEM, including incidents relating to product defects, OEM-controlled service availability, security incidents, or other failures within the OEM's scope of responsibility. The requirement for submission of the RCA report within three (3) working days from the date of incident resolution shall apply to Severity 1 and Severity 2 incidents. For Severity 3 and lower-severity incidents, where an RCA is required by the Bank, the same shall be provided within a timeline mutually agreed between the Bank/Bidder and the OEM, or within the timeline prescribed by the applicable regulator/regulatory authority, as amended from time to time, whichever is earlier. The above clarification shall not relieve the respective solution OEM of its obligation to provide necessary technical assistance, investigation support and incident analysis where the root cause is initially unclear or requires joint investigation.
1022	87 / 138 / 221	7.16 OEM Services & Deployment (Architecture Assessment) / 12.2 / Annexure 8	Clause 7.16 item 4 read with Annexure 8 clause 1(c) and Clause 12.2	Clause 7.16 item 4 lists the solutions for which the OEM architecture assessment is to be conducted from Year 2 as SIEM, SOAR, UEBA and XDR only. Annexure 8 clause 1(c) applies the annual configuration/architecture review obligation to every OEM, and Clause 12.2 provides an 'Architecture Assessment' payment milestone against submission of a report and presentation to the Bank's senior management on a yearly basis.	We request you to please confirm the definitive list of OEMs required to deliver the annual architecture assessment, and to confirm that a corresponding priced line exists in Appendix 2 (Commercial Bill of Material) for every such OEM. If the obligation is intended to apply to all 14 solution OEMs and nine service OEMs, We request you to please to align Clause 7.16 item 4 accordingly.	Annual OEM Architecture Assessment, including submission of an Architecture Assessment Report and presentation to the Bank's senior management, shall apply to the OEMs/solutions specifically identified under Clause 7.16, Item 4, namely SIEM, SOAR, UEBA and XDR. The corresponding commercial treatment shall be as provided in Appendix 2 – Commercial Bill of Material. However, this clarification does not relieve other solution/service OEMs from their obligations under the RFP. Each OEM shall, as applicable to its proposed solution/service, conduct the required configuration, architecture, health and performance review, identify configuration or architectural gaps, risks, optimization opportunities and deviations from recommended practices, and provide the Bank with the necessary technical guidance, recommendations and support for optimization, hardening and improvement of the respective solution/service throughout the contract period inline with the scope defined in the RFP.
1023	222-223	Annexure 8: Certification on OEM Requirements	Annexure 8 clause 5 (Cloud-Hosted Solution Confirmation)	'We confirm that all OEM and CSP commitments, obligations and dependencies required under this RFP have been secured and incorporated through appropriate agreements, support commitments, contractual arrangements and other binding mechanisms, as applicable.'	An OEM cannot contractually flow down to a hyperscale CSP obligations such as physical audit of data centres by the Bank or its regulators (Cloud Deployment Requirement S.No. 11 and 31.2). We request you to please confirm that this undertaking is limited to obligations within the OEM's own control and to those CSP commitments available under the CSP's standard enterprise agreement and published compliance programme, and to permit the OEM to qualify the undertaking to that effect without it being treated as a conditional compliance.	Please refer addendum for revised clause
1024	163 / 220 / GeM bid	14.14 Make in India / Annexure 7: Minimum Local Content Certification / GeM bid	Clause 14.14 read with Annexure 7 and GeM bid 'MII Compliance: Yes'	Clause 14.14 refers to the Public Procurement (Preference to Make in India) Order 2017, including the revision dated 19.07.2024, whereas Annexure 7 still cites the revision dated 04.06.2020. The GeM bid records MII Compliance = Yes and MSE Purchase Preference = Yes, but the bid documents do not state the applicable minimum local-content threshold or purchase-preference class.	We request you to please confirm (a) the governing PPP-MII order/revision and the applicable minimum local-content threshold and purchase-preference class (Class-I / Class-II local supplier) for this procurement; (b) the basis for computing local content for subscription SaaS contracted through an India-registered entity, hosted in an India cloud region and supported/delivered from India; and (c) whether Annexure 7 certification is required only from the Bidder/local supplier or separately from each solution/service OEM.	No Change, Please be guided by the RFP
1025	101-128 / GeM bid	10.2 Eligibility Evaluation Criteria / GeM bid 'Documents required from seller'	GeM bid: 'OEM Authorization Certificate, OEM Annual Turnover'	The GeM bid document (GEM/2026/B/8018719) lists 'OEM Annual Turnover' among the documents required from the seller. Clause 10.2 (Eligibility Evaluation Criteria) and Clause 10.3 (Technical Evaluation Criteria) do not prescribe any OEM turnover criterion, threshold or evaluation weightage.	We request you to please to specify whether an OEM annual turnover threshold applies and, if so, (a) the threshold amount, (b) the financial years to be considered, (c) whether it is to be met by the OEM's global parent entity or its India entity, and (d) whether it applies to all 14 solution OEMs and nine service OEMs or only to specified solutions. If no OEM turnover criterion is intended, We request you to please to issue a corrigendum on GeM removing this document requirement.	The turnover criteria mentioned in the RFP is for Bidder's only
1026	101-102	10.2 Eligibility Evaluation Criteria	Criterion 5 - Manufacturer's Authorization Form (MAF)	MAF is required from 14 solution OEMs and 9 service OEMs, on the OEM's official letterhead signed by an authorised signatory having the authority to bind the OEM.	We request you to please confirm that (a) where a single OEM provides more than one of the listed solutions and/or services, one consolidated MAF listing all such solutions and services is acceptable; (b) the MAF may be issued by the OEM's India entity where that entity is the contracting, licensing and support entity, supported by a group authorisation; and (c) a single MAF may be issued jointly to the Bidder and its authorised distributor where the OEM transacts through a distributor in India.	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1027	132-133	10.3 Technical Evaluation Criteria	Criterion 6 - OEM services implemented in Client (BFSI/PSU/PSE/Govt Organization) in India	Up to 9 marks, 1 mark per service, requiring credentials for each of Breach Attack & Simulation, Continuous Automated Red Teaming, Attack Surface Management, Phishing Simulation, Anti-Phishing, Dark Web Monitoring, Brand Protection & Monitoring, Threat Intelligence Feed and Threat Hunting Services.	We request you to please confirm the acceptable forms of evidence where client identities are subject to confidentiality obligations - specifically whether (a) a masked client reference with the client category and scope certified by the OEM, (b) an OEM self-declaration listing client names in a sealed/confidential annexure accessible only to the evaluation committee, or (c) a client email confirmation, will be accepted; and whether credentials of the OEM's India entity and its group entities may be cited jointly.	Please refer the Section10.2 Eligibility Evaluation Criteria. The documents requriement remains same for the technical evalaution as well.
1028	169 / Appendix 1A Instructions	15.1 to 15.3 APPENDIX 1A/1B/1C / Appendix 1A 'Instructions' sheet	Clause 15.1-15.3 read with Appendix 1A Instructions items 1 to 5 and Clause 10.3	Appendix 1A/1C score each requirement as S = 10 and C = 3 and state that a response other than S/C is deemed N and may make the bid liable for rejection. Clause 10.3 separately allocates the 100 technical marks across bidder experience (30 marks), solution-OEM experience (51 marks), service-OEM experience (9 marks) and technical presentation (10 marks), with no separate weightage shown for Appendix 1A/1C compliance scores.	We request you to please to clarify: (a) whether the 'Respective Solution Compliance (%)' / Appendix 1A/1C calculated scores are pass/fail compliance indicators only, or whether they affect the 100-mark technical score under Clause 10.3; (b) whether a single N response against any line item results in rejection of the entire bid, or whether rejection applies only to mandatory/non-negotiable requirements; and (c) whether any minimum per-sheet or overall S/C compliance percentage applies, and if so, the threshold and calculation method.	Any N/non-compliant response shall lead to rejection. Bidder to comply with the FRS specificied in the RFP.
1029	Appendix 1A Instructions	Appendix 1A - Instructions sheet	Instructions item 4	Responses are limited to 'S' (Standard) or 'C' (Customization); any other response is deemed 'N' and renders the bid liable for rejection.	Several line items are architecturally inapplicable to a given deployment model - for example Bank-hosted N+N HA and dual management console requirements for a pure-SaaS service, email security gateway requirements in the Anti-Phishing Services sheet, and infrastructure controls in the Cloud Deployment Requirement sheet for OEM-owned SaaS. We request you to please to introduce a 'Not Applicable (NA)' response option, with a mandatory justification field, so that items which are inapplicable by reason of the mandated deployment model are excluded from both the numerator and the denominator of the compliance score rather than being scored as non-compliance.	No Change, Please be guided by the RFP. The response options in Funtional Requirement sheet shall remain limited to “S” (Standard) and “C” (Customization) as specified in the RFP. Any response other than “S” or “C” shall be treated as “N” (Non-Compliant) and may render the bid liable for rejection in accordance with the RFP
1030	Appendix 1A Instructions	Appendix 1A - Instructions sheet	Instructions item 1	'Bidder must mandatorily mention the exact page number & clause or section reference from their submitted technical proposal or OEM product documentation which demonstrate compliance with each criteria (specification). Any Response marked as compliance without a valid page reference/section reference, shall be treated as in-complete and may be liable for rejection/scoring penalties.'	For Managed Services and SaaS platforms, capability is documented in OEM service descriptions, datasheets and online product documentation rather than in installable product manuals. We request you to please confirm that a reference to the OEM's service description, datasheet, online documentation URL, or an OEM-signed capability statement on letterhead submitted as an annexure to the technical bid, constitutes a valid reference for the purpose of Instruction item 1.	The bidder shall mandatorily provide an exact page number and clause/section reference from the documents submitted as part of the technical bid to substantiate compliance with each criterion. For Managed Services, SaaS and other cloud-delivered solutions, the relevant capability can be documented/ highlighted through OEM service descriptions, datasheets, product/service documentation or official online documentation. Where an OEM-signed capability statement is submitted, it shall clearly identify the relevant RFP requirement and confirm the capability of the specific product/service/version proposed. The Bank reserves the right to seek clarification or supporting evidence where the submitted reference does not adequately establish compliance. The bidder shall remain responsible for ensuring that all references provided are accurate, current and verifiable.
1031	Appendix 1A	Appendix 1A - Functional Compliance Sheet (Solutions)	Sheet: Threat Inteligence Platform (TIP), S.No. 24 and 35	S.No. 24: '...The detection should be retrospective and allows the analyst to search back in seconds without going back to the SIEM solution... The retention is bounded to the POV period.' S.No. 35: '...For POV purposes we will integrate with the SIEM solution.'	S.No. 24 and S.No. 35 refer to a 'POV period', whereas this procurement is for a production deployment. We request you to please to clarify the intended production requirement for these line items and to specify the required historical intelligence retention period so that OEMs can size and price retention consistently.	The reference to “POV period” shall be read in the context of the production deployment. The solution shall support configurable expiry/retention of threat intelligence indicators and retrieval/restoration of historical threat-intelligence data for investigation and forensic requirements as specified in the RFP for the complete duration of the contract.
1032	Appendix 1A / 45	Appendix 1A - Sheet: Threat Inteligence Platform (TIP) read with Clause 7.3.7	Sheet TIP S.No. 4 and 14 read with Clause 7.3.7	S.No. 4: 'The solution should integrate up to multiple sources of threat intelligence required by the organization into a single management platform without any extra cost. The Sources should either be part of the Intelligence Channels, or Commercial sources that the client is subscribed to.' S.No. 14: 'The solution should offer a wide range of commercial CTI providers out of the box, including atomic IOCs, threat bulletins, and any other threat intelligence offered by each provider.'	We request you to please confirm (a) the commercial threat intelligence subscriptions the Bank already holds and intends to onboard into the TIP, and (b) whether the TIP OEM is required to supply any commercial intelligence content itself, or only the platform and the connectors for Bank-subscribed sources and the separately procured Threat Intelligence Feed under Clause 7.4.7. This determines whether intelligence content is priced once (under the Threat Intelligence Feed line) or twice.	a) bidder as a part of holistic solution required to factored in "TIF" i.e commercial as well as OSINT and same is to be integrated with proposed "TIP" b) TIP is required to be integrated with TIF any parsers, intelligence, connectors etc. required is to be factored in by the bidder
1033	137-138	12.1 Product (Software) Cost	12.1, items 1 and 3 (Product License Cost / Subscription Cost)	Payment of Product Licence Cost and Subscription Cost is 50% 'On successful delivery of the licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware', supported by 'Delivery proof', 'OOTB Installation Proof' and 'Invoice of the Product'; 20% on UAT sign-off; 30% on Go-Live.	For SaaS, 'delivery' is typically tenant provisioning/activation rather than installation on Bank hardware. We request you to please confirm the acceptable documentary evidence that will substitute for OOTB installation proof for SaaS subscriptions and Managed Services, and to clarify whether the commercial subscription term/billing starts from tenant activation or from Go-Live. If tenant activation is required before Go-Live for implementation or UAT, please confirm how that interim period is to be treated commercially.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1034	138 / 98	12.1 Product (Software) Cost / 8 Contract Period	12.1 Note (Subscription Licensing Model) read with Clause 8	For the Subscription Licensing Model, the Subscription Renewal Charges for Year-4 and Year-5 shall be quoted separately in the Commercial Bill of Material and shall be payable from the fourth year onwards.' Clause 8 provides for Implementation Period plus a Support period of 60 months post Go-Live, extendable by up to two years.	We request you to please confirm the intended subscription structure - namely that the quoted Subscription Cost covers Years 1 to 3 from Go-Live and that Year-4 and Year-5 are quoted as separate annual renewals - and to confirm the reference date from which each subscription year runs (Go-Live date, or date of tenant provisioning). Bank is further requested to confirm the basis on which the two-year extension will be priced for subscription services, given that Clause 8 caps extension pricing at 120% of the last year's AMC/ATS/Facility Management rates.	Clarification: ***For Subscription Licensing Model,*** the bidder shall quote the applicable Subscription Cost and separately quote the Annual Subscription Renewal Charges, as prescribed in the Commercial Bill of Material. The subscription period shall commence from the respective Go-Live date of the solution/service. Tenant provisioning prior to Go-Live shall not, by itself, constitute commencement of the contractual subscription period. The Subscription Cost/Subscription Renewal Charges shall include the applicable OEM support, updates, upgrades, patches, bug fixes, security updates, maintenance and other obligations specified under the RFP for the respective subscription period ***For Perpetual or other non-subscription software*** licensing models, the bidder shall quote the applicable ATS charges separately, as prescribed in the RFP. The applicable OEM support, updates, upgrades, patches, bug fixes and maintenance obligations shall be provided in accordance with the quoted ATS and the RFP. The Bank may, at its sole discretion, extend the contract/ support services for up to two (2) additional years, in one-year increments, in accordance with Clause 8 of the RFP. Such
1035	140	12 Payment Terms	12.6 Note (undertaking from OEM on outstanding amounts)	'The Bidder shall submit, prior to the release of each payment during the O&M phase, an undertaking signed by respective OEM confirming that there are no outstanding or overdue amounts payable by the Bidder in respect of the proposed solution(s) and services under this RFP.'	We request you to please confirm the frequency and format of this OEM undertaking, preferably aligned to the applicable O&M payment cycle, and that it is required only from the OEMs whose solution or service is the subject of that particular payment, so that the obligation remains administratively workable across the multiple solution/service OEMs over the five-year term.	Please be guided by the provisions of the RFP. The OEM undertaking shall be submitted prior to the release of each O&M payment, from the respective OEM(s) whose solution(s)/service(s) are covered under the invoice raised by the Bidder for that particular payment. Further, the Bank may, on an ad hoc basis and at its discretion, require the Bidder to submit such OEM undertaking(s) prior to the release of any O&M payment or any other payment due to the Bidder under the RFP. In such cases, the Bidder shall obtain and submit the requisite undertaking(s) from the concerned OEM(s) to the Bank prior to release of the respective payment.
1036	136	11 Right to Reduce / Descope Solution Components Prior to Award	Clause 11	The Bank reserves the right to descope one or more Solution Components, Modules, Licences, Services, Quantities or IT Infrastructure items at any stage prior to issuance of the Contract/Letter of Award, and such descope 'shall not create any liability or obligation towards the Bidder'.	OEM subscription pricing is volume-linked and is quoted on the basis of the published sizing. We request you to please confirm that, where the volumetrics or scope of a service are reduced at award, (a) bidders may submit volume-linked pricing bands in the Commercial Bill of Material, or (b) the price for the reduced scope will be derived pro rata from the quoted unit rates, rather than the originally quoted lump sum being held applicable to a reduced scope.	Please refer the addendum for revised clause
1037	26-27 / 58	7.1 Scope and Objectives / 7.5 Bidder Responsibilities	Clause 7.1 (paragraph on customisation) and Clause 7.6.8	'Any customization, enhancement, parser development, connector creation, workflow automation, dashboard customization, incident integration, playbook development, reporting customization, alert tuning, remediation activities, APIs, or native integrations required for successful implementation shall be provided without any additional cost to the Bank throughout the contract period.'	As drafted the obligation is unbounded and cannot be estimated or priced by an OEM over a five-year term. We request you to please confirm a governance mechanism - for example an annual allowance of OEM effort-days per solution/service for enhancements and new integrations, with requirements beyond that allowance addressed through a mutually agreed change-control process at pre-agreed rates - so that the obligation is bounded while the Bank retains assured capacity.	No Change, Please be guided by the RFP
1038	66	7.6.7 Training	Clause 7.6.7 and the training table	Per proposed solution/OEM: Beginner/Foundation training of 2 days per session x 5 sessions; Advanced/Administrator training of 3 days per session x 5 sessions; Backend Administration, Troubleshooting & Maintenance training of 3 days per session x 5 sessions - i.e. 40 instructor-days per OEM. In addition, certification of 15 Bank officials with the relevant Cloud Service Provider covering Cloud Security, Threat Hunting, Detection Engineering, Cloud Incident Response & Forensics and Threat Intelligence & CTI Analysis, within 12 months of Go-Live, failing which Liquidated Damages apply.	We request you to please confirm: (a) the number of participants per session and whether the same participants may attend multiple levels; (b) whether the 40 instructor-day programme applies to each of the 14 proposed solution OEMs and, separately, whether any equivalent mandatory training/session count applies to the nine offsite service OEMs; (c) for SaaS solutions with a single administrative console, whether role-based foundation/advanced/administration training may be consolidated where all prescribed learning outcomes are covered; (d) whether the separate certification of 15 Bank officials from the relevant CSP is required only for the CSP hosting the SIEM, as stated in the clause, and whether certification examination fees are to be included; and (e) whether OEM-led virtual instructor training is acceptable where the OEM's standard certification programme is delivered remotely.	Please refer addendum for revised clause
1039	147	13.1 Service Level Agreement - Services SLAs	Services SLAs: 'Anti-phishing, Anti-rogue app, anti-malware etc. / Brand protection and Monitoring / Dark Web Monitoring', item (a) and the Penalty column	'a. Detection of phishing sites, rogue app, brand abuse, malicious content etc. elaborated in RFP > 85%.' Penalty: 'Non-detection or late detection - Rs. 1 Lakh each for non-detection or late detection of phishing site, anti-rogue, malware, social media, mobile app, etc.'	A detection-rate service level requires a defined and knowable denominator; threats that are not detected by any party cannot be enumerated, and 'late detection' is not defined. We request you to please to (a) define the measurement basis - for example, the percentage of phishing/brand-abuse incidents reported to the Bank through any channel during the month that had already been detected and notified by the service within a defined detection window; (b) define 'late detection' by reference to a measurable detection window from first observability; (c) confirm the monthly cap on the aggregate penalty under this head; and (d) confirm that incidents relating to assets, brands or domains outside the agreed monitored scope are excluded.	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1040	147	13.1 Service Level Agreement - Services SLAs	Services SLAs items (b) and (c) and the Penalty column	'b. Site take-down time for identified Phishing URLs - Resolution within 24 hours. c. Site take-down time for Brand Abuse - Resolution within 36 hours.' Penalty: 'Rs.5000/- for every hour beyond resolution time.'	Completion of a takedown is dependent on third parties outside the service provider's control, including registrars, registries, hosting providers, application marketplaces, social-media platforms, browser vendors and, in some jurisdictions, law enforcement. We request you to please to distinguish between provider-controlled activities and third-party completion by defining committed timelines for incident validation, takedown initiation and escalation, while treating actual third-party takedown completion as a target supported by ageing/escalation reporting. Alternatively, please confirm that time awaiting action by the relevant third party is excluded from the SLA clock and associated hourly penalty.	No Change, Please be guided by the RFP
1041	148	13.1 Service Level Agreement - Services SLAs	Services SLAs items (d), (e) and (f)	'd. Enrichment: Cybercrime - Resolution within 1 Hours. e. Enrichment: Nation State - Resolution within 1 Hours. f. Any other (Like Interaction, Ransomware, Malware Reverse Engineering etc.) - Resolution within 1 Hours (From the time of reporting the request/issue through phone call/email/web-based portal).'	Malware reverse engineering, threat-actor interaction and nation-state attribution are analyst-led investigative activities whose completion time depends on scope and complexity. We request you to please to define 'Resolution' for each category and establish tiered, measurable timelines for acknowledgement/triage, preliminary enrichment and final analysis/reporting, rather than a single one-hour completion requirement. Please also specify the monthly volume of such requests included within the service and the mechanism for requests beyond that volume.	No Change, Please be guided by the RFP
1042	147	13.1 Service Level Agreement - Services SLAs	'Each Proposed Services Uptimes - 99.90%'	'For every 0.05% or part thereof drop in service levels penalty will be 1% of the Monthly Maintenance Cost. Service level drop below 90%, penalty shall amount to 100% of the Monthly Maintenance Cost.'	We request you to please to clarify (a) the measurement method for SaaS/managed-service uptime and agreed exclusions (scheduled maintenance approved/notified in advance, force majeure, Bank-caused outages, and third-party systems/connectivity outside the service provider's control); (b) how the 'Monthly Maintenance Cost' formula on page 146 is to be applied to an uptime breach of one individual SaaS/managed service - specifically, whether the penalty base will be the monthly value attributable to that affected service rather than the project-wide aggregate MMC; and (c) whether uptime penalties are recovered only against payment amounts attributable to the affected service, subject to the overall penalty cap in Clause 13.2.	No Change, Please be guided by the RFP
1043	157-158 / 165	13.2 Penalties / 13.3 At-Risk Amount / 14.21 Limitation of Liability	Clause 13.2, 13.3 and 14.21	Clause 13.2 caps total penalties under LD and SLA at 10% of the overall contract value. Clause 13.3 sets the monthly At-Risk Amount at 15% of the estimated monthly payout. Clause 14.21 caps aggregate liability at the total Project Cost.	We request you to please confirm that (a) the Rs. 1 lakh per-instance detection penalty and the Rs. 5,000 per hour takedown penalty at Clause 13.1 fall within, and are not additional to, the 10% cap at Clause 13.2; (b) penalties attributable to a specific solution or service are computed on, and limited to, the contract value of that solution or service rather than the overall contract value; and (c) where liability is passed through to an OEM, the OEM's aggregate liability is limited to the value of that OEM's own solution and services under the contract.	No Change, Please be guided by the RFP
1044	98-99 / 157	9 PROJECT TIMELINES / 13.2 Penalties	Clause 9 read with Clause 13.2 (Liquidated Damages - Installation & Implementation)	Overall implementation period of 5 months from T0 for all solutions and services; LD of 1% per week or part thereof of the respective Product Cost, subject to a maximum of 10% of total contract value; and 'If the LD due to Implementation of the respective product cost/existing product cost reaches 25% of the implementation cost of the respective product/services, the bidder is required to replace the product/services.'	We request you to please confirm that (a) LD in respect of an individual solution or service is computed on that solution's or service's cost and is not levied where delay is attributable to Bank-side dependencies (availability of data sources and log feeds, confirmation of the monitoring seed list and asset scope, approvals, network/firewall changes, UAT scheduling and stakeholder availability) or to a dependency on another OEM's deliverable; and (b) the milestone dates for each solution and service in the Bank-issued Project Plan will be agreed with the respective OEM, given that onboarding effort differs materially between an on-premises platform and a SaaS subscription.	No Change, Please be guided by the RFP
1045	159	14.1 Assignment & Subcontracting	Clause 14.1	The selected bidder shall not subcontract/JV/Consortium or permit anyone to perform any of the work, service or other performance required under the contract (excluding Proposed OEM personnels). All bidder personnel proposed for the Bank shall be on the Bidder's payroll.	We request you to please confirm that delivery/support by a proposed OEM through its disclosed group entities, affiliates or OEM-controlled delivery/research centres does not constitute prohibited subcontracting, provided such personnel operate under the proposed OEM's responsibility and governance, the contracting OEM remains fully accountable under its MAF/Annexure 8 undertaking, and all applicable Bank approvals, data-residency, access-control, privacy and security obligations are met.	No Change, Please be guided by the RFP
1046	7 / GeM bid	1 KEY INFORMATION / GeM bid document GEM/2026/B/8018719	'Last Date for submission of Pre-Bid Query: 15/09/2026 at 5:00 PM' and 'Date and Time for Pre-Bid Meeting: 16/09/2026 at 11:00 AM'	The GeM bid document records the Pre-Bid date and time as 11-09-2026 09:00:00 (Online), whereas the RFP states the pre-bid query deadline as 15/09/2026 5:00 PM and the pre-bid meeting as 16/09/2026 11:00 AM.	We request you to please confirm the operative pre-bid query deadline and pre-bid meeting date and time, and to publish a corrigendum on the GeM portal aligning the GeM bid schedule with the RFP, so that bidders and their OEMs are not prejudiced by the discrepancy.	No Change, Please be guided by the RFP
1047	Appendix 1C	Appendix 1C - Functional Compliance Sheet (Services)	Sheet: Dark Web Monitoring, S.No. 24	'Monitor MX, SPF, DKIM and DMARC changes for suspicious domains.'	We request you to please to clarify that this requirement is limited to externally observable DNS/email-authentication intelligence for suspicious/look-alike domains. MX, SPF and DMARC records can be monitored through public DNS; comprehensive DKIM monitoring requires knowledge or discovery of the selector and cannot be guaranteed for every third-party domain. Please confirm that monitoring of publicly observable records and known/discovered DKIM selectors will be treated as compliant.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1048	Appendix 1C / 147	Appendix 1C Functional Compliance / 13.1 Services SLA	Dark Web Monitoring S.No. 52; Brand abuse S.No. 7 and 16; Clause 13.1 takedown SLA	The RFP requires takedown licences from Day One, unlimited takedowns during the contract period, and 24/36-hour takedown completion targets.	We request you to please to clarify that 'unlimited takedowns' means no cap on valid, in-scope takedown initiation and coordination during the contract period, subject to Bank approval and the policies/processes of registrars, registries, hosting providers, app stores, social platforms and other relevant third parties. Please also define eligible takedown asset categories and confirm that assets for which no actionable abuse basis exists, including parked/inactive domains or cases where the responsible third party will not act, are excluded from guaranteed completion.	No Change, Please be guided by the RFP. The term “unlimited takedowns” shall mean that there shall be no contractual numerical cap on valid, in-scope takedown requests initiated and coordinated by the Bidder during the contract period, subject to the Bank's approval/authorization and the applicable scope of the service. The Bidder shall maintain appropriate records of all takedown requests, including identification of the asset, basis for takedown, date/time of detection and submission, third-party response, follow-up actions and closure status, and shall provide such records to the Bank as required.
1049	Appendix 1C	Appendix 1C - Functional Compliance Sheet (Services)	Anti-Phishing S.No. 22-23; Brand abuse S.No. 16	APWG membership; global partnerships with domain registrars/application distribution platforms/ISPs; and 'tie-ups' with browser providers and CERT-In for blocking/takedown.	We request you to please confirm whether these criteria may be satisfied collectively by the proposed OEM, Bidder and/or an authorised takedown/response partner, and whether documented operational escalation, abuse-reporting and blocklist-submission channels with registrars, app stores, browsers and CERT-In are acceptable in lieu of formal bilateral 'tie-up' agreements.	Please refer addendum for revised clause.
1050	Appendix 1A p.57	Appendix 1A - Functional Compliance Sheet (Solutions)	Threat Inteligence Platform (TIP), S.No. 10	TIP should provide an out-of-box Threat Intelligence Playbook library, OR integrate with a third-party solution for IOC hunting, IOC dissemination, IOC-to-vulnerability mapping etc.; if a third party is required it must be provided and integrated at no additional cost.	SOAR is already being procured as a separate solution under this RFP. We request you to please confirm that standards-based/API/connector integration of the TIP with the selected SOAR and the relevant SIEM/vulnerability-management platforms may be used to implement IOC hunting, dissemination and IOC-to-vulnerability workflows, without requiring the TIP OEM to bundle a second orchestration product at no additional cost.	Bidder to meet the requirment as mentioned in the RFP .
1051	Appendix 1A p.58	Appendix 1A - Functional Compliance Sheet (Solutions)	Threat Inteligence Platform (TIP), S.No. 23-24	TIP should enable rapid detection/response of matches within the environment and retrospective matching/search without going back to the SIEM; S.No. 24 also refers to a POV retention period.	We request you to please to clarify what Bank telemetry or security data is expected to be ingested into the TIP for 'matches within the environment' and retrospective search. Where production telemetry remains in the Bank's SIEM/XDR, please confirm that bidirectional TIP-SIEM/SOAR integration, IOC matching and retrospective correlation using the Bank's telemetry platforms will meet the required outcome, rather than requiring the TIP to duplicate SIEM telemetry storage/search.	The reference to “POV period” shall be read in the context of the production deployment. The solution shall support configurable expiry/retention of threat intelligence indicators and retrieval/restoration of historical threat-intelligence data for investigation and forensic requirements as specified in the RFP for the complete duration of the contract.
1052	Appendix 1A p.58	Appendix 1A - Functional Compliance Sheet (Solutions)	Threat Inteligence Platform (TIP), S.No. 34, 36 and 37	Multi-analyst collaboration on the same ticket/case; downstream synchronisation using minimum-confidence filters and indicator tags.	We request you to please confirm that integration with the Bank's selected ITSM/SOAR platform through supported APIs/connectors may satisfy collaborative case handling and confidence/tag-based downstream actioning where those workflow functions are not native to the TIP, provided the required end-to-end outcome is demonstrated.	Bidder to meet the requirment as mentioned in the RFP .
1053	261	16.21 Annexure 21: Sizing/Volumetrics, Data Retention and Current Infrastructure	16.21.2 Volumetrics - Solution-wise Requirements, S.No. 16 CTEM	CTEM volumetrics state: Vulnerability/Exposure Findings - Unlimited; Attack Paths/Exposure Relationships - Unlimited; Users/Endpoints - 12,000 scalable to 16,000; IPs - 4,000.	The Appendix 1A CTEM compliance sheet is predominantly an agentless external exposure/digital-risk specification, while Clause 7.3.14 describes a VM+BAS-led CTEM scope. We request you to please to clarify what 'Users/Endpoints' and 'IPs' represent for CTEM licensing/sizing (internal endpoints, external IPs/assets, identities or another metric), and to publish the authoritative Day-1 and scale target for domains/subdomains, external IPs, brands, executives and related entities after the CTEM scope conflict is resolved.	No Change, Please be guided by the RFP
1054	35 of 122	XDR	4.13	The goal is to minimize the attack surface by continuously monitoring, updating, and provide compensatory controls for vulnerabilities and exploits in the endpoints	We request to modify this clause as below "The goal is to minimize the attack surface by continuously monitoring, updating, and provide visibility for vulnerabilities and exploits in the endpoints" Justification: The term "visibility" is outcome-focused and technology-agnostic, allowing solutions to detect and report vulnerabilities through various mechanisms (signatures, behavioral analysis, real-time scanning, etc.), whereas "compensatory controls" is overly prescriptive and implies specific mitigation techniques that may not be applicable to all vulnerability types or endpoint environments. Changing to "visibility" maintains the security intent while enabling bidders to propose diverse, fit-for-purpose solutions without unnecessary implementation constraints.	No Change, Please be guided by the RFP
1055	35 of 122	XDR	12	The proposed solution must provide protection against malicious AI application tampering on the endpoints	We request to modify this clause as below "The proposed solution must provide protection against malicious applications tampering on the endpoints" Justification:The "AI" qualifier is overly specific and may exclude non-AI malware threats, creating coverage gaps. The broader term "malicious application tampering" aligns with industry-standard endpoint protection language and ensures comprehensive threat protection regardless of the attack vector or technology employed.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1056	36 of 122	XDR	15	The proposed XDR solution must provide comprehensive activity data management and search capabilities, including receiving activity data in the form of telemetry, and metadata; feature for automatic query runs and email notifications; threat matching features using Boolean Logic and other criteria; and options to export, import, delete, and share saved search queries.	We request to modify this clause as below: The proposed XDR solution must provide comprehensive activity data management and search capabilities, including receiving activity data in the form of telemetry, and metadata; feature for automatic query runs and email notifications; threat matching features using Boolean Logic and other criteria; and options to export, delete, and share saved search queries. Justification:The "import" functionality is not a core operational requirement for XDR activity data management. The primary requirements are exporting queries for backup/sharing, deleting obsolete queries, and sharing queries among team members—all of which are standard XDR capabilities. Import functionality introduces unnecessary complexity, potential security/governance risks from external query sources, and is not universally supported across commercial XDR solutions, thereby limiting vendor options unnecessarily	No Change, Please be guided by the RFP
1057	36 of 122	XDR	22	The solution should offer options to leverage anti-malware and anti-spyware components stored locally on agents, or signatures stored in-the-vendor cloud	From the operational context and use cases for each deployment option, ensuring continuity of threat protection in all connectivity scenarios. By explicitly defining "when offline" (local components) and "when online" (cloud signatures), the clause reconsiders ambiguity regarding the solution's capability to maintain protective coverage during network disconnections while leveraging updated threat intelligence when connectivity is available We request to modify this clause as below "The solution should offer options to leverage anti-malware and anti-spyware components stored locally on agents when offline, or signatures stored in-the-vendor cloud when online."	No Change, Please be guided by the RFP
1058	36 of 122	XDR	29	The solution Device Control capability must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The solution Device Control capability must support Network Devices, USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, time based device control capabilities allowing admin to define the policy specifically for the endpoint operating systems (Windows 10, 11 or higher).	We request to modify the clause as below: The solution Device Control capability must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The solution Device Control capability must support USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, allowing admin to define the policy specifically for the endpoint operating systems (Windows 10, 11 or higher)to allow the devices as required. Justification: Network Devices are typically managed through enterprise network security controls and firewalls rather than endpoint Device Control, and time-based controls create unnecessary operational complexity and maintenance overhead. The modified clause focuses on high-risk local device vectors (USB, Mobile Storage, Bluetooth, Modems) that pose direct security threats to endpoints, while allowing flexibility for organizations to enable specific devices based on business requirements.	No Change, Please be guided by the RFP
1059	37 of 122	XDR	43	The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature or through seamless integration with a third-party sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data	We request to amend this clause as below: The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data. Justification: To ensure operational independence and reduce implementation complexity, the organization requires native sandbox functionality built into the core solution rather than relying on third-party integrations, which introduce external dependencies, potential single points of failure, and increase support overhead. This modification mandates that bidders deliver complete sandboxing capability as an integrated component from day 1, ensuring seamless functionality, consistent vendor accountability, and simplified maintenance and support operations without external vendor coordination.	Please refer addendum for revised Clause
1060	38 of 122	XDR	57	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	We request to amend this clause as below: The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture or 99.9% availability SLA distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead. Justification: The modification provides architectural flexibility while maintaining the Bank's core availability objective. Not all qualified SaaS vendors employ Active-Active multi-AZ architecture; however, industry-standard 99.9% SLA meets enterprise-grade requirements and enables broader vendor participation without compromising operational resilience. This alternative approach is vendor-agnostic, measurable, and backed by contractual guarantees rather than architectural prescriptions.	Please refer Addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1061	37 of 122	XDR	42	The proposed solution should provide recommended actions to address and mitigate threats detected on endpoints. These remediation suggestions should be informed by forensic data collected from endpoints and detailed analysis performed by the solution to enhance threat response and resolution.	To ensure accurate cost proposals and licensing calculations, please clarify the estimated forensics data volume requirements: a) What is the expected monthly forensics data volume (in GB) that the solution must support? b) What is the planned retention period for forensics data? c) Does this volume include forensics data from all sources (endpoints, servers, cloud workloads, network) or specific sources only? This clarification will enable all bidders to calculate appropriate licensing models and provide consistent cost estimates	Details shall be shared with the successful bidder
1062	Addition of Point as recommendation	Cloud Security	To be Added in Cloud Security	The proposed solution should also support the File scanning with no limitation on file/object type or size covering application across organisation. This should include but is not limited to Amazon Simple Storage Service (S3), Amazon FSx amd Amanzon Elastic File System.	Benefit to PSB: Comprehensive file scanning eliminates critical security blind spots across the organization's cloud storage infrastructure, ensuring no malware, ransomware, or sensitive data can be inadvertently stored in S3, FSx, or EFS without detection. By removing file type and size limitations, the solution prevents attackers from bypassing scanning through obfuscation or leveraging uncommon formats, while the multi-storage coverage consolidates security posture across diverse AWS storage services under a single unified policy. This provides unified threat visibility, enables regulatory compliance (HIPAA, PCI-DSS, GDPR), prevents data exfiltration, and protects against insider threats and supply chain compromises affecting cloud-stored data—significantly reducing the risk of ransomware attacks, compliance violations, and unauthorized data exposure.	No Change, Please be guided by the RFP
1063	page 30 of 273	Extended Detection & Response (XDR)	5	Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Cloud (SaaS): HA Deployment aligned with the SLA, RTO & RPO (Refer Section 13). Management Console: Deployed at both Primary and Secondary sites	We request to amend this clause as below: Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Cloud (SaaS): HA Deployment aligned with the SLA, RTO & RPO (Refer Section 13). Justification: In Appendix 1A clause 27 under XDR explicitly mention for SaaS "ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead" Though it's a SaaS based the management console cannot be deployed at both primary and secondary sites.	Please refer addendum for revised clause
1064	page 31 of 273	Cloud Workload Protection Platform (CWPP)	13	Cloud (SaaS): Deployment aligned with the SLA, RTO & RPO (Refer Section 13).. Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Management Console: Deployed at both Primary and Secondary sites	We request to amend this clause as below: Cloud (SaaS): Deployment aligned with the SLA, RTO & RPO (Refer Section 13).. Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Justification: For SaaS solution the management console cannot be deployed at banks primary & secondary site	Please refer addendum for revised clause
1065	Page 38 of 122 & Page 38 of 122	XDR	22 to 35	These points are duplicate need to be removed	These points are duplicate and need to be reconsiderd	No Change, Please be guided by the RFP
1066	23	SIEM / Functional Specification	23	Where a native parser or connector is unavailable, the proposed solution shall provide supported mechanisms, SDKs, APIs, templates, or configuration interfaces to develop and maintain custom integrations	For a recuced overall TCO and ensure the timely availability without any delay, please rephrase it to: OEM /OEM authorized partner to provide parsers for data ingestion for all the current data sources and their respective upgrades (in maximum 15 business days from data of intimation of the same) during the contract period. If any new data source is added during the contract period, the OEM will provide parsers for data ingestion in maximum 15 business days from data of intimation of the same, without dependency of the bidder.	No Change, Please be guided by the RFP
1067	28	SIEM / Incident Response	131	The proposed cloud-delivered solution shall provide secure multi-tenant architecture with appropriate logical tenant isolation, encryption in transit and at rest, secure authentication, MFA, granular RBAC, audit logging and protection of Bank security data in accordance with the approved service architecture, security controls and SLA.	Why there is a need for multi-tennacy, this is specially required in a service provider environment needing multiple customers to be managed, please reconsider or rephrase it to: The proposed solution must provide fine grained role-based access into actions and assets, so users can be granted with investigative actions and not containment actions."	Please refer the addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1068	59	7.6 OEM Responsibilities	1.	All activities relating to solution architecture, design, implementation, configuration, customization, integration, migration, testing, deployment, documentation, training, and Go-Live shall be performed by the respective Solution OEM in coordination with the Bidder	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: 1. All activities relating to solution architecture, design, implementation, configuration, customization, integration, migration, testing, deployment, documentation, training, and Go-Live shall be performed by the respective Solution OEM /OEM authorized partner in coordination with the Bidder. 2. The OEM /OEM authorized partner shall design, implement, and support an enterprise-grade, scalable, resilient, secure, and future-ready solution compatible with the Bank's existing and target IT and Cyber Security architecture across on-premises, cloud, and hybrid environments. 3. The OEM /OEM Authorized partner shall prepare and submit all design documents including HLD, LLD, deployment architecture, integration architecture, configuration guides, SOPs, operational manuals, as-built documentation, and implementation artefacts. 4. The OEM /OEM authorized partner shall provide all native and custom integrations, APIs, connectors, parsers, workflows, playbooks, dashboards, reports, automation, authentication, authorization, RBAC, logging, monitoring, alerting, and interoperability required for successful operation of the solution. 5. The OEM /OEM authorized partner shall perform sizing validation, deployment, migration, configuration, tuning, optimization, health checks, and stabilization to ensure	Please refer addendum for revised clause
1069	60	7.16 OEM Services & Deployment (Architecture Assessment)	87	Assessment & performance review 1. Review of respective solutions configurations (Custom parsers, playbooks, controls, rules and process etc.) of the OEM solution 2. System Optimization review and suggestion including remedial actions. 3. Review the bidder's implementation of suggestions of remedial actions. 4. List of Solution for which Assessment is to be conducted, Year 2 Onwards are	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: OEM /OEM authorized partner for Services & Deployment (Architecture Assessment) Assessment & performance review 1. Review of respective solutions configurations (Custom parsers, playbooks, controls, rules and process etc.) of the OEM solution 2. System Optimization review and suggestion including remedial actions. 3. Review the bidder's implementation of suggestions of remedial actions. 4. List of Solution for which Assessment is to be conducted, Year 2 Onwards are	No Change, Please be guided by the RFP
1070	60	7.6.1 Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder)		Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder) Requirement Analysis - Activities are to be performed by Respective Solution OEM/OEM Authorized Partner (supported by bidder) 1. The respective Solution OEM, assisted by the bidder, shall conduct a detailed assessment of the Bank's business, functional, technical, operational, security, compliance, and integration requirements and design a scalable, resilient, and futureready solution. The proposed solution shall fully comply with the requirements specified in the RFP and support future business and technology needs of the Bank. 2. As part of the requirement gathering phase, the OEM shall conduct workshops, discovery sessions, interviews, and discussions with the Bank's stakeholders and appointed consultants to understand business requirements, existing infrastructure & solutions, integrations, operational processes, and security requirements. 3. The OEM shall review the Bank's existing IT, security, application, network, cloud, and infrastructure landscape and recommend an optimized target-state architecture leveraging both existing and proposed components wherever feasible.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner Requirement Analysis - Activities are to be performed by Respective Solution OEM/OEM Authorized Partner (supported by bidder) 1. The respective Solution OEM /OEM authorized partner, assisted by the bidder, shall conduct a detailed assessment of the Bank's business, functional, technical, operational, security, compliance, and integration requirements and design a scalable, resilient, and futureready solution. The proposed solution shall fully comply with the requirements specified in the RFP and support future business and technology needs of the Bank. 2. As part of the requirement gathering phase, the OEM/OEM authorized partner shall conduct workshops, discovery sessions, interviews, and discussions with the Bank's stakeholders and appointed consultants to understand business requirements, existing infrastructure & solutions, integrations, operational processes, and security requirements. 3. The OEM /OEM authorized partner shall review the Bank's existing IT, security, application, network, cloud, and infrastructure landscape and recommend an optimized target-state architecture leveraging both existing and proposed components wherever feasible. 4. The OEM /OEM authorized parrtner but not be limited to: a. Requirements elicitation and analysis	No Change, Please be guided by the RFP
1071	61	7.6.2 System Design - Activities are to be performed by Respective solution OEM (supported by bidder)	7.6.2	System Design - Activities are to be performed by Respective solution OEM 1. The bidder and respective OEM shall be responsible for the end-to-end design, sizing, customization, configuration, integration, implementation, deployment, maintenance, and support of the proposed solution, including coordination with all associated OEMs, service providers, and stakeholders. 2. All proposed NextGEN SOC solutions shall support seamless interoperability, realtime integration, event sharing, correlation, orchestration, and automated response capabilities to enable unified security operations and minimize manual intervention. 3. The proposed solution shall be configurable and customizable to meet the Bank's functional, technical, operational, reporting, security, and compliance requirements. 4. The bidder and OEM shall design and implement a secure, scalable, resilient, and future-ready architecture based on the approved requirements, data flows, integrations, and operational needs of the Bank. 5. The bidder and OEM shall prepare and submit the following design documents for Bank approval: a. High-Level Design (HLD), including solution	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner System Design - Activities are to be performed by Respective solution OEM/OEM authorized partner (supported by bidder) 1. The bidder and respective OEM /OEM authorized partner shall be responsible for the end-to-end design, sizing, customization, configuration, integration, implementation, deployment, maintenance, and support of the proposed solution, including coordination with all associated OEMs, service providers, and stakeholders. 2. All proposed NextGEN SOC solutions shall support seamless interoperability, realtime integration, event sharing, correlation, orchestration, and automated response capabilities to enable unified security operations and minimize manual intervention. 3. The proposed solution shall be configurable and customizable to meet the Bank's functional, technical, operational, reporting, security, and compliance requirements. 4. The bidder and OEM/OEM authorized partner shall design and implement a secure, scalable, resilient, and future-ready architecture based on the approved requirements, data flows, integrations, and operational needs of the Bank. 5. The bidder and OEM/OEM authorized partner shall prepare and submit the following design documents for Bank approval: a. High-Level Design (HLD), including solution architecture, deployment architecture, integration architecture, and data flow	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1072	61	7.6.3 Development and Installation - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.6.3	1. All installation, configuration, customization, testing, migration, integration, UAT, GoLive, and related implementation activities shall be performed from the Bank's premises. 2. The bidder and respective OEM shall integrate the proposed solution with the Bank's ITSM, SLA Monitoring, monitoring, logging, authentication, and other enterprise platforms, as required. 3. The bidder and OEM shall coordinate with all relevant third parties, OEMs, service providers, and Bank stakeholders to ensure seamless integration, interoperability, and end-to-end functionality of the proposed solution. 4. The bidder shall provide all required integrations, connectors, parsers, APIs, workflows, playbooks, dashboards, reports, alerts, fine-tuning, customizations, enhancements, and remediation activities necessary for successful operation of the solution throughout the contract period without any additional cost to the Bank. 5. The bidder shall adopt and submit an implementation methodology covering solution deployment, customization, testing, managed services, facility management services, knowledge transfer, and hardware/software installation and configuration activities.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Development and Installation - Activities are to be performed by Respective Solution OEM /OEM authorized partner(supported by bidder) 1. All installation, configuration, customization, testing, migration, integration, UAT, GoLive, and related implementation activities shall be performed from the Bank's premises. 2. The bidder and respective OEM/OEM authorized partner shall integrate the proposed solution with the Bank's ITSM, SLA Monitoring, monitoring, logging, authentication, and other enterprise platforms, as required. 3. The bidder and OEM /OEM authorized partner shall coordinate with all relevant third parties, OEMs, service providers, and Bank stakeholders to ensure seamless integration, interoperability, and end-to-end functionality of the proposed solution. 4. The bidder shall provide all required integrations, connectors, parsers, APIs, workflows, playbooks, dashboards, reports, alerts, fine-tuning, customizations, enhancements, and remediation activities necessary for successful operation of the solution throughout the contract period without any additional cost to the Bank. 5. The bidder shall adopt and submit an implementation methodology covering solution deployment, customization,	No Change, Please be guided by the RFP
1073	62	7.6.4 Documentation - Activities are to be performed by Respective solution OEM (supported by bidder	7.6.4	The bidder and respective OEM shall prepare, maintain, obtain Bank approval/sign-off, and submit all project, technical, operational, security, and administrative documentation associated with the proposed solution. The indicative list of deliverables shall include, but not be limited to, the following: 1. Detailed Project Plan and Implementation Plan 2. Hardware, Software, Infrastructure, and Sizing Specifications 3. High-Level Design (HLD) and Low-Level Design (LLD) Documents 4. Solution Architecture, Deployment Architecture, and Data Flow Documents 5. Secure Configuration Standards, Baseline Hardening Documents, and Security Configuration Guides 6. System, Database, Integration, Troubleshooting, Diagnostics, and Maintenance Documents 7. Testing, Validation, Acceptance, and Go-Live Documents 8. Change Management, Release Management, Problem Management, and Operational Procedures 9. User Management, Access Management, and Role Administration Guides 10. Release Notes, Impact Assessment Matrix, and Dependency Mapping Documents	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Documentation - Activities are to be performed by Respective solution OEM/OEM authorized partner (supported by bidder The bidder and respective OEM shall prepare, maintain, obtain Bank approval/sign-off, and submit all project, technical, operational, security, and administrative documentation associated with the proposed solution. The indicative list of deliverables shall include, but not be limited to, the following: 1. Detailed Project Plan and Implementation Plan 2. Hardware, Software, Infrastructure, and Sizing Specifications 3. High-Level Design (HLD) and Low-Level Design (LLD) Documents 4. Solution Architecture, Deployment Architecture, and Data Flow Documents 5. Secure Configuration Standards, Baseline Hardening Documents, and Security Configuration Guides 6. System, Database, Integration, Troubleshooting, Diagnostics, and Maintenance Documents 7. Testing, Validation, Acceptance, and Go-Live Documents 8. Change Management, Release Management, Problem Management, and Operational Procedures 9. User Management, Access Management, and Role Administration Guides 10. Release Notes, Impact Assessment Matrix, and Dependency	No Change, Please be guided by the RFP
1074	63	7.6.5 Deployment and Go-Live - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.6.5	1. The bidder and respective OEM shall be responsible for deployment of the solution in the production environment, Go-Live planning, implementation, installation, configuration, fine-tuning, migration, stabilization, and hyper care support. 2. The bidder and OEM shall provide onsite support during the hyper care period, monitor solution performance, assist users, conduct training sessions, address issues and defects, implement corrective actions, and recommend operational best practices. 3. The implementation scope shall include deployment planning, migration, testing, validation, issue resolution, user acceptance support, Go-Live execution, and postGo-Live stabilization activities. 4. Prior to Go-Live, the solution shall undergo security validation activities, including VAPT, IS Audit, readiness assessments, identification of security gaps and blind spots, risk remediation, and implementation of recommendations. The Bank or its appointed agency may conduct Continuous Automated Red Teaming, Purple Teaming, security assessments, or other validation exercises as deemed necessary. 5. The bidder and OEM shall conduct performance testing prior to UAT and Go-Live to validate that the	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Deployment and Go-Live - Activities are to be performed by Respective Solution OEM /OEM authorized partner (supported by bidder) 1. The bidder and respective OEM/OEM authorized partner shall be responsible for deployment of the solution in the production environment, Go-Live planning, implementation, installation, configuration, fine-tuning, migration, stabilization, and hyper care support. 2. The bidder and OEM /OEM authorized partner shall provide onsite support during the hyper care period, monitor solution performance, assist users, conduct training sessions, address issues and defects, implement corrective actions, and recommend operational best practices. 3. The implementation scope shall include deployment planning, migration, testing, validation, issue resolution, user acceptance support, Go-Live execution, and postGo-Live stabilization activities. 4. Prior to Go-Live, the solution shall undergo security validation activities, including VAPT, IS Audit, readiness assessments, identification of security gaps and blind spots, risk remediation, and implementation of recommendations. The Bank or its appointed agency may conduct Continuous Automated Red Teaming, Purple Teaming, security assessments,	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1075	64	7.6.6 Testing- Activities are to be performed by Respective solution OEM (supported by bidder)	7.6.6	1. The Bank shall conduct User Acceptance Testing (UAT) to validate that the proposed solution and all associated components, integrations, workflows, reports, dashboards, and functionalities comply with the requirements specified in the RFP, approved FRSM/SRS, and other project documents. 2. The bidder and respective OEM shall confirm completion of all implementations, configuration, customization, integration, migration, and testing activities prior to commencement of UAT and certify that the solution is ready for user validation. 3. The bidder shall provision and maintain dedicated Development, Testing, UAT, and Pre-Production environments throughout the contract period. All software, licenses, and other resources required for such environments shall be included within the bidder's scope without any additional cost to the Bank. 4. Any defects, deviations, vulnerabilities, observations, or non-compliances identified during UAT, security assessments, audits, reviews, or validation exercises shall be rectified by the bidder within the timelines prescribed by the Bank and at no additional cost. 5. The bidder shall maintain appropriate version control, configuration management, change	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Testing- Activities are to be performed by Respective solution OEM/OEM authorized partner (supported by bidder) 1. The Bank shall conduct User Acceptance Testing (UAT) to validate that the proposed solution and all associated components, integrations, workflows, reports, dashboards, and functionalities comply with the requirements specified in the RFP, approved FRSM/SRS, and other project documents. 2. The bidder and respective OEM /OEM authorized partner shall confirm completion of all implementations, configuration, customization, integration, migration, and testing activities prior to commencement of UAT and certify that the solution is ready for user validation. 3. The bidder shall provision and maintain dedicated Development, Testing, UAT, and Pre-Production environments throughout the contract period. All software, licenses, and other resources required for such environments shall be included within the bidder's scope without any additional cost to the Bank. 4. Any defects, deviations, vulnerabilities, observations, or non-compliances identified during UAT, security assessments, audits, reviews, or validation exercises shall be rectified by the bidder within the timelines prescribed by the Bank and at no additional cost.	No Change, Please be guided by the RFP
1076	65	7.6.6.1 Quality Assurance	7.6.6.1	1. Testing Requirements a. The respective OEM shall be responsible for planning, executing, documenting, and successfully completing all testing activities required to validate the functionality, performance, stability, reliability, security, interoperability, and operational readiness of the proposed solution. The bidder shall prepare detailed test plans, test cases, test data, automation scripts (where applicable), entry and exit criteria, test reports, defect logs, root cause analysis reports, workarounds, and remediation plans, and shall obtain the Bank's approval wherever required. 2. Test Preparation The respective OEM shall: a. Prepare the overall testing strategy and methodology for Unit Testing (UT), UAT, Performance Testing, Security Testing, and other applicable tests. b. Establish and maintain the required test environments, infrastructure, software, applications, and test data. c. Prepare, validate, and execute test cases, scripts, and automation frameworks, wherever applicable. d. Define test entry and exit criteria, acceptance criteria, and success parameters. 3. Test Execution The respective OEM shall: a. Execute all approved test cases and scripts. b. Record, track, report, and resolve defects,	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: 1. Testing Requirements a. The respective OEM/OEM authorized partner shall be responsible for planning, executing, documenting, and successfully completing all testing activities required to validate the functionality, performance, stability, reliability, security, interoperability, and operational readiness of the proposed solution. The bidder shall prepare detailed test plans, test cases, test data, automation scripts (where applicable), entry and exit criteria, test reports, defect logs, root cause analysis reports, workarounds, and remediation plans, and shall obtain the Bank's approval wherever required. 2. Test Preparation The respective OEM /OEM authorized partner shall: a. Prepare the overall testing strategy and methodology for Unit Testing (UT), UAT, Performance Testing, Security Testing, and other applicable tests. b. Establish and maintain the required test environments, infrastructure, software, applications, and test data. c. Prepare, validate, and execute test cases, scripts, and automation frameworks, wherever applicable. d. Define test entry and exit criteria, acceptance criteria, and success parameters. 3. Test Execution The respective OEM /OEM authorized partner	No Change, Please be guided by the RFP
1077	66	7.6.7 Training- Activities are to be performed by Respective solution OEM (supported by bidder)	7.6.7	7.6.7 Training- Activities are to be performed by Respective solution OEM (supported by bidder) The bidder and respective OEMs shall provide comprehensive product training, knowledge transfer, and certification programs for the Bank's IT and Information Security personnel at no additional cost. All technical and product-specific training shall be delivered by OEM. Upon successful completion of the training programs, the respective OEM shall issue participation and/or certification certificates to the attendees. The bidder shall submit a detailed Training and Certification Plan covering training objectives, curriculum, skill levels, training schedules, participant eligibility, certification pathways, and assessment criteria. The training program shall cover product functionalities, administration, troubleshooting, maintenance, security best practices, automation, advanced threat scenarios, security monitoring and analysis, incident response and investigation, threat detection and hunting, intelligence analysis, new features, upgrades, operational workflows, and relevant industry trends. Bidder along with the OEM should provision the training & certification of the bank's relevant officials from the relevant Cloud service provider where the	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Training- Activities are to be performed by Respective solution OEM /OEM Authorized partner (supported by bidder) The bidder and respective OEMs /OEM authorized partner shall provide comprehensive product training, knowledge transfer, and certification programs for the Bank's IT and Information Security personnel at no additional cost. All technical and product-specific training shall be delivered by OEM/OEM Authorized partner. Upon successful completion of the training programs, the respective OEM /OEM Authorized partner shall issue participation and/or certification certificates to the attendees. The bidder shall submit a detailed Training and Certification Plan covering training objectives, curriculum, skill levels, training schedules, participant eligibility, certification pathways, and assessment criteria. The training program shall cover product functionalities, administration, troubleshooting, maintenance, security best practices, automation, advanced threat scenarios, security monitoring and analysis, incident response and investigation, threat detection and hunting, intelligence analysis, new features, upgrades, operational workflows, and relevant industry trends. Bidder along with the OEM/OEM authorized partner should provision the training & certification of the bank's relevant officials from the relevant	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1078	67	7.6.8 Security requirements - Activities are to be performed by Respective solution OEM (supported by bidder)	7.6.8	1. The bidder and respective OEMs shall comply with the Bank's IT, Information Security, Cyber Security, Data Protection, Privacy, Business Continuity, and related policies, standards, procedures, and guidelines, as shared by the Bank from time to time. The bidder shall be responsible for ensuring the confidentiality, integrity, availability, security, and privacy of the Bank's information assets, systems, applications, and data throughout the contract period. 2. The bidder shall implement and maintain appropriate administrative, technical, physical, and operational controls for protection of data, applications, systems, infrastructure, and associated assets under its custody or management. 3. The bidder shall comply with the Bank's requirements relating to access management, privileged access management, password policies, user administration, data protection, encryption, monitoring, incident management, and security governance. 4. The bidder shall ensure encryption and protection of data at rest, data in transit, and data in use, wherever applicable, using industry-standard security controls and cryptographic mechanisms. All tools, technologies, and controls required to achieve the same shall form part of the proposed solution.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Security requirements - Activities are to be performed by Respective solution OEM/OEM authorized partner (supported by bidder) 1. The bidder and respective OEMs/OEM authorized partner shall comply with the Bank's IT, Information Security, Cyber Security, Data Protection, Privacy, Business Continuity, and related policies, standards, procedures, and guidelines, as shared by the Bank from time to time. The bidder shall be responsible for ensuring the confidentiality, integrity, availability, security, and privacy of the Bank's information assets, systems, applications, and data throughout the contract period. 2. The bidder shall implement and maintain appropriate administrative, technical, physical, and operational controls for protection of data, applications, systems, infrastructure, and associated assets under its custody or management. 3. The bidder shall comply with the Bank's requirements relating to access management, privileged access management, password policies, user administration, data protection, encryption, monitoring, incident management, and security governance. 4. The bidder shall ensure encryption and protection of data at rest, data in transit, and data in use, wherever applicable, using	No Change, Please be guided by the RFP
1079	70	7.7 On-cloud proposed solution OEM Responsibilities	7.6.9	1. The security telemetry received by the OEM Cloud platform will be routed to the dedicated tenant/workspace provisioned for the Bank.	What is the requirement here, is it required to maintain a copy of all cloud data to a local instance /data lake, please clarify, who need to provision this, does bank has this instance available, if not required please reconsider this ask.	The security telemetry received and processed by the OEM Cloud/SaaS platform shall be logically segregated and maintained within a dedicated tenant/workspace provisioned for the Bank. The dedicated tenant/workspace shall ensure segregation of the Bank's security data, configurations, policies, analytics, alerts, incidents and other Bank-related information from those of other customers.
1080	71	7.10 Data Privacy	7.1 0	Executive Governance and Project Oversight 1. The bidder and each respective OEM shall nominate a senior executive as the Project Sponsor/Project Director responsible for executive governance, stakeholder management, escalation management, strategic oversight, and overall project success. 2. The Project Sponsor, Project Director, and designated senior representatives of the bidder and OEMs shall participate in governance meetings, executive reviews, strategy workshops, and escalation meetings as required by the Bank. An, On quarterly/or as per the frequency defined by bank, executive governance meetings shall be conducted throughout the contract period to review project progress, service delivery, operational performance, security posture, compliance, risks, technology enhancements, and continuous improvement opportunities. 3. The bidder and OEMs shall deploy and maintain adequately skilled, certified, experienced, and qualified resources, together with appropriate backup resources, succession planning, and skill development mechanisms, to ensure uninterrupted 24x7x365 service delivery throughout the contract period.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Executive Governance and Project Oversight 1. The bidder and each respective OEM/OEM authorized partner shall nominate a senior executive as the Project Sponsor/Project Director responsible for executive governance, stakeholder management, escalation management, strategic oversight, and overall project success. 2. The Project Sponsor, Project Director, and designated senior representatives of the bidder and OEMs /OEM authorized partner shall participate in governance meetings, executive reviews, strategy workshops, and escalation meetings as required by the Bank. An, On quarterly/or as per the frequency defined by bank, executive governance meetings shall be conducted throughout the contract period to review project progress, service delivery, operational performance, security posture, compliance, risks, technology enhancements, and continuous improvement opportunities. 3. The bidder and OEMs /OEM Authorized partner shall deploy and maintain adequately skilled, certified, experienced, and qualified resources, together with appropriate backup resources, succession planning, and skill development mechanisms, to ensure uninterrupted 24x7x365 service delivery throughout the contract period. 4. The bidder shall establish and maintain a Bank-approved	Please refer addendum for revised clause
1081	72	7.12 Resource Requirement	7.6.12	7.12.1Implementation Phase • Prior to commencement of implementation, the bidder and respective OEMs shall submit a detailed Resource Deployment Plan for Bank approval identifying proposed onsite and offsite resources, roles, responsibilities, certifications, experience, deployment schedules, and solution-wise allocation. • The bidder shall deploy a dedicated onsite Project Manager throughout the implementation phase and nominate appropriate bidder and OEM resources for each solution, workstream, milestone, and project activity. • Any replacement, redeployment, or modification of approved implementation resources shall require prior written approval from the Bank.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Implementation Phase • Prior to commencement of implementation, the bidder and respective OEMs /OEM authorized partner shall submit a detailed Resource Deployment Plan for Bank approval identifying proposed onsite and offsite resources, roles, responsibilities, certifications, experience, deployment schedules, and solution-wise allocation. • The bidder shall deploy a dedicated onsite Project Manager throughout the implementation phase and nominate appropriate bidder and OEM /OEM authorized partner resources for each solution, workstream, milestone, and project activity. • Any replacement, redeployment, or modification of approved implementation resources shall require prior written approval from the Bank.	No Change, Please be guided by the RFP
1082	72	7.12.2Operations and Maintenance (O&M) Phase		7.12.2Operations and Maintenance (O&M) Phase • The bidder shall deploy the minimum onsite L1, L2, Project Manager/L3 – Operations, and other resources specified in the RFP and ensure uninterrupted 24x7x365 support through an appropriate shift-based deployment model. • The respective OEMs shall provide subject matter experts from the date of installation throughout the contract period to support operations, troubleshooting, optimization, upgrades, audits, vulnerability remediation, and major incidents. • The bidder shall ensure adequate SME support for timely resolution of incidents, service requests, problems, vulnerabilities, and operational issues.	O & M shall be bidders responsibility pleaase reconsider OEM from this to maintain right availability and cost Operations and Maintenance (O&M) Phase • The bidder shall deploy the minimum onsite L1, L2, Project Manager/L3 – Operations, and other resources specified in the RFP and ensure uninterrupted 24x7x365 support through an appropriate shift-based deployment model. • The respective bidder shall provide subject matter experts from the date of installation throughout the contract period to support operations, troubleshooting, optimization, upgrades, audits, vulnerability remediation, and major incidents. • The bidder shall ensure adequate SME support for timely resolution of incidents, service requests, problems, vulnerabilities, and operational issues.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1083	73	7.12.3Resource Management and Governance	7.12	OEM Implementation Resources Onsite (Full Time) OEM shall submit a detailed resource deployment plan before commencement of requirement gathering. Any replacement or modification shall require prior Bank approval.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: OEM /OEM authorized partner Implementation Resources Onsite (Full Time) OEM/OEM authorized partner shall submit a detailed resource deployment plan before commencement of requirement gathering. Any replacement or modification shall require prior Bank approval.	No Change, Please be guided by the RFP
1084		7.17 System recovery	1	. In case of disaster, it is the responsibility of the Respective solution OEM along with the bidder to ensure that services remain unaffected and same is up and running from secondary site (DR)	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: . In case of disaster, it is the responsibility of the Respective solution OEM/OEM Authorized partner along with the bidder to ensure that services remain unaffected and same is up and running from secondary site (DR)	No Change, Please be guided by the RFP
1085		7.19 Other In-Scope Services	7.19	7.19.1Other Scope Activity 1. The Respective solution OEM along with the bidder is expected to ensure that all functionalities as mentioned in Appendix 1A: Functional Specification are made available to PSB. 2. The Respective solution OEM along with the bidder is expected to ensure that for the purpose of this RFP, statutory and regulatory changes shall mean any change prescribed by the statutory and regulatory bodies governing/ affecting the banking industry in India viz. Reserve Bank of India, Ministry of Finance, CCIL, NPCI, IBA, SEBI, or any such bodies constituted by the RBI mandating change/s to an existing functionality of the Solution shall be provided to the Bank at no additional cost for the entire contract period. However, any Statutory and Regulatory changes post Go-Live of the respective applications (which are not a part of the existing functionalities) will be on CR basis based on the rates provided in the Bill of Material. 3. The Respective Solution OEM along with the bidder is expected to carry out a requirement study for the functionalities and services required by PSB, to gain understanding of the business requirements. 4. Respective solution OEM along with the bidder	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: 1Other Scope Activity 1. The Respective solution OEM/OEM Authorized partner along with the bidder is expected to ensure that all functionalities as mentioned in Appendix 1A: Functional Specification are made available to PSB. 2. The Respective solution OEM/OEM Authorized partner along with the bidder is expected to ensure that for the purpose of this RFP, statutory and regulatory changes shall mean any change prescribed by the statutory and regulatory bodies governing/ affecting the banking industry in India viz. Reserve Bank of India, Ministry of Finance, CCIL, NPCI, IBA, SEBI, or any such bodies constituted by the RBI mandating change/s to an existing functionality of the Solution shall be provided to the Bank at no additional cost for the entire contract period. However, any Statutory and Regulatory changes post Go-Live of the respective applications (which are not a part of the existing functionalities) will be on CR basis based on the rates provided in the Bill of Material. 3. The Respective Solution OEM/OEM Authorized partner along with the bidder is expected to carry out a requirement study for the functionalities and services required by PSB, to gain understanding of the business requirements. 4. Respective solution OEM /OEM Authorized partner along	Please refer addendum for revised clause
1086		7.19.4DR Setup - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.19.4	DR Setup - Activities are to be performed by Respective Solution OEM (supported by bidder) 1. Respective solution OEM along with the bidder has to ensure that DR setup is ready on the date of Go Live of respective Applications 2. Respective solution OEM along with the bidder should make necessary setup to enable the DR within the agreed timelines. 3. Respective solution OEM along with the bidder should carry out the deployment of the application in DC and DR, UAT as applicable. 4. To ensure proper rollback, Respective solution OEM along with the bidder has to ensure that the old setup at all the locations is as–IS as per the agreed timelines during migration strategy formulation	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner DR Setup - Activities are to be performed by Respective Solution OEM /OEM authorized partner (supported by bidder) 1. Respective solution OEM /OEM Authorized partneralong with the bidder has to ensure that DR setup is ready on the date of Go Live of respective Applications 2. Respective solution OEM/OEM Authorized partner along with the bidder should make necessary setup to enable the DR within the agreed timelines. 3. Respective solution OEM/OEM Authrized partner along with the bidder should carry out the deployment of the application in DC and DR, UAT as applicable. 4. To ensure proper rollback, Respective solution OEM/OEM Authrized partner along with the bidder has to ensure that the old setup at all the locations is as–IS as per the agreed timelines during migration strategy formulation	No Change, Please be guided by the RFP
1087		13 SERVICE LEVELS & PENALTIES	2	2. The bidder and the OEM shall be jointly responsible for the maintenance, configuration, performance, and fault-free operation of the entire supplied infrastructure, including hardware, software, operating systems, databases, and related components, during the warranty, AMC, ATS, and FMS periods, as applicable	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: The bidder and the OEM /OEM authorized partner shall be jointly responsible for the maintenance, configuration, performance, and fault-free operation of the entire supplied infrastructure, including hardware, software, operating systems, databases, and related components, during the warranty, AMC, ATS, and FMS periods, as applicable	No Change, Please be guided by the RFP
1088	159	14.1 Assignment & Subcontracting	1	The selected bidder shall not subcontract/JV/Consortium or permit anyone to perform any of the work, service or other performance required under the contract (excluding Proposed OEM personnels). All bidder's personnel proposed for the bank shall be on bidder's Payroll. Bank will seek relevant documentation from the bidder to validate the same.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: The selected bidder shall not subcontract/JV/Consortium or permit anyone to perform any of the work, service or other performance required under the contract (excluding Proposed OEM /OEM Autorized partner personnels). All bidder's personnel proposed for the bank shall be on bidder's Payroll. Bank will seek relevant documentation from the bidder to validate the same.	No Change, Please be guided by the RFP
1089	30	RFP - 7.2 Solution & Services Deployment Model and Their HA Requirement 7.2.1 Solutions – Master Deployment Matrix	6. Network Detection & Response (NDR)	Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Management Console: Deployed at both DC and DR	Different NDR solution works on different redundancy deployment methodology (I.e Active - Active or Active - Passive). Request bank to modify the clause as: Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active/Passive at DC and HA, N+N, Active-Active/Passive at DR. Management Console: Deployed at both DC and DR	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1090	45	RFP - Scope of Work 7.3.5 Network detection and response (NDR)	7.3.5.1 Modules, Architecture & Deployment:	Pt 2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Generally NDR solutions are deployed with sole purpose of doing network analysis, threat detection & response and does not have native 2FA capability, so request bank to remove this point. As an alternate as proposed in same point, proposed NDR solution can be integrated with bank's existing MFA solution.	Please refer addendum for the revised clause
1091	49	RFP - Scope of Work 7.3.10 Application security testing Tool	7.3.10.1 Modules, Architecture & Deployment:	Pt 2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Generally AST solutions are deployed with sole purpose of scanning the source code, web, api etc and does not have native 2FA capability, so request bank to remove this point. As an alternate as proposed in same point, proposed AST solution can be integrated with bank's existing MFA solution.	No Change, Please be guided by the RFP
1092	260	RFP - 16.21.2 Volumetrics- Solution-wise Requirements	12. Application Security Testing Tool	All the inline components of the solution must operate in high availability mode. In the event of any component failure, the system should automatically initiate failovers within seconds, ensuring uninterrupted functionality without requiring manual intervention.	Application Security Testing as a technology in general works at developemnt/pre-production/UAT stage only. And hence as a solution there is no need of high availability mode. Same has already been updated in this RFP (as solution is asked in standalone at both DC & DR). So, request bank to reconsiderd this clause.	Please refer addendum for the revised clause
1093	40	APPENDIX 1A Functional Compliance Sheet (Solutions)	Network Detection & Response (NDR)	Pt 8. Proposed solution should generate a root cause analysis, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets.It should provide a platform for easier investigation like visual graphical view and timeline of the attack and it should support tagging of MITRE tactics, techniques and procedures used by the attacker in alerts and incidents.	We reqeust bank to amend the clause: Proposed solution should generate a root cause analysis / incident management, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets.It should provide a platform for easier investigation like visual graphical view and timeline of the attack and it should support tagging of MITRE tactics, techniques and procedures used by the attacker in alerts and incidents.	Please refer addendum for the revised clause
1094	40	APPENDIX 1A Functional Compliance Sheet (Solutions)	Network Detection & Response (NDR)	Pt 13. The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	As bank has asked for on-premise solution for NDR, on the contrary, this clause asks for cloud-native SAAS ask. So, we kindly request bank to reconsider this clause.	Please refer Addendum for revised clause
1095	42	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 3. The solution must be able to analyse a wide array of programming languages including Java,.Net, C/C++, Objective-C, Android, PHP, COBOL, Ruby, Swift, HTML 5, Scala, APEX, TypeScript, Go, Kotlin and ABAP etc but not limited to these alone	Considering the future requirements of AI in Secure Code Development and most of the development is moving towards AI generated code using AI supported languages. So it is very important for bank to have coverage around this as well and will recommend to incorporate AI supported languages like "R, Ada, Solidity, Bash, Groovy, Rust, Perl", but not limited to these alone.	No Change, Please be guided by the RFP
1096	42	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 24. Solution should support Machine learning and Analysis based on the archived results	ML capability is important, but it is very important to have coverage around AI based code as well. And will recommend bank to consider: The solution should have the capability to scan AI generated code. The solution should be able to integrate with AI coding agent via MCP	No Change, Please be guided by the RFP
1097	43	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 32. The solution should be able to support Composition Analysis: Identify the opens source components used in the application. Vulnerabilities & outdated version Licensing risk associated with the components	Bank is looking for Software composition analysis and asked for identifying the open source component and licensing risk. But this limited information is not enough for bank to secure themselves with rapidly increasing supply chain attacks and we will highly recommend to consider following as well: SCA system must catalogue open source components from Maven, NPM, and Nuget. SCA system has to be able to generate a Bill of Materials for an application. Solution should have the ability to continuously monitor the scanned components & notify if there are any zero day attacks without performing the rescan. Solution should Catalog, Store, and Audit SBOMs (both cycloneDx & SPDX) generated for in-house developed software applications and COTS applications.	No Change, Please be guided by the RFP
1098	55–56	7.4.3 Attack surface management	7.4.3	The Bidder shall provide continuous discovery, monitoring, classification, and risk assessment of the Bank's external and internal attack surface. Discovery of internet-facing and internal assets.	Considering that the ASM Managed Service covers both the Bank's external and internal attack surfaces, please confirm that complementary OEM technologies/tools may be utilized, as required, for delivery of the respective external and internal attack-surface requirements, while collectively meeting all stated requirements of the ASM Managed Service for the Bank's external and internal attack surface.	Please refer Addendum for revised clause
1099	56	7.4.3 Attack surface management	7.4.3	Discovery of internet-facing and internal assets. Identification of exposed services, applications, APIs, domains, cloud assets, certificates, and digital infrastructure.	Please confirm that discovery of the internal attack surface shall include maintaining a consolidated inventory of internal cyber assets by aggregating and correlating available asset and configuration information across supported on-premises, cloud, identity, endpoint, network and security environments.	Please refer Addendum for revised clause
1100	56	7.4.3 Attack surface management	7.4.3	Continuous exposure monitoring. Identification of misconfigurations and security exposures.	Please confirm that internal attack-surface monitoring shall include current and historical asset/configuration visibility and identification of relevant configuration changes, deviations and drift, including visibility of the previous and current configuration state, what changed and when.	No Change, Please be guided by the RFP. Bank is looking for external attack surface management

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1101	56	7.4.3 Attack surface management	7.4.3	Continuous exposure monitoring. Risk prioritization based on business impact.	Please confirm that internal attack-surface monitoring shall support predefined and Bank-defined metrics, monitoring criteria, thresholds and compliance-relevant conditions/rules for relevant asset, configuration, security and operational attributes, including conditions aligned to applicable Bank-defined security standards, policies and configuration baselines, with configurable change detections, alerts and reporting for identified deviations.	No Change, Please be guided by the RFP. Bank is looking for external attack surface management
1102	55–56	7.4.3 Attack surface management	7.4.3	The Bidder shall provide continuous discovery, monitoring, classification, and risk assessment of the Bank's external and internal attack surface. Continuous exposure monitoring.	Please confirm that internal attack-surface monitoring shall maintain time-stamped historical asset, configuration and change information for at least 12 months, with facility to review historical states and changes for investigation, audit readiness, control validation and compliance-assurance purposes.	No Change, Please be guided by the RFP. Bank is looking for external attack surface management
1103	56	7.4.3 Attack surface management	7.4.3	Discovery of internet-facing and internal assets. Identification of exposed services, applications, APIs, domains, cloud assets, certificates, and digital infrastructure.	Please confirm that internal attack-surface visibility shall include supported network and network-security assets and relevant available configuration information, including device, interface, VLAN, firewall, NAT, VPN and certificate information, where available and applicable to the respective supported technology, for identifying relevant configuration deviations and security exposures.	Please refer Addendum for revised clause
1104	56	7.4.3 Attack surface management	7.4.3	Identification of misconfigurations and security exposures. Recommendations for attack surface reduction.	Please confirm that identified internal configuration/exposure conditions may be re-evaluated following remediation during a subsequent applicable assessment/data-collection cycle, to validate whether the identified condition continues to exist.	No Change, Please be guided by the RFP. Bank is looking for external attack surface management
1105	32	7.2.2 Services	7.2.2	Attack Surface Management (ASM) — Managed Service; Continuous / 24×7 monitoring; Weekly discovery/update; Monthly reporting.	Please confirm that the internal attack-surface capability shall provide centralized search, filtering, dashboards, visualizations and reports across relevant asset, identity, configuration, change and available security/risk information, with facility to export relevant information/evidence for use in the ASM Managed Service's prescribed weekly discovery/update and monthly reporting cycle.	No Change, Please be guided by the RFP
1106	32	7.2.2 Services	7.2.2	Attack Surface Management (ASM) — Managed Service; Continuous / 24×7 monitoring; Weekly discovery/update; Monthly reporting.	Please confirm that one or more complementary OEM technologies/tools may be utilized for delivery of the complete ASM Managed Service, providing the respective external and internal attack-surface requirements, while collectively meeting all applicable ASM Managed Service requirements.	No Change, Please be guided by the RFP
1107	102, 120–123	Eligibility Criteria	Eligibility Criteria / OEM Requirements	MAF should also be submitted from the following services OEMs: 3. Attack Surface management	Where complementary OEM technologies/tools are utilized for delivery of the complete ASM Managed Service, please confirm that separate MAFs are required to be submitted by the respective OEMs for the external and internal attack-surface management services requirements.	No Change, Please be guided by the RFP
1108	54–55	7.4 Functional Requirement - Services (Offsite Services)	7.4	The Bidder shall ensure compliance with all applicable Government of India guidelines, RBI directives, CERT-In advisories, regulatory requirements, and the Bank's policies relating to data localization, data privacy, data sharing, and information security. All tools/platforms proposed for delivery of these services shall comply with the Bank's applicable information security, data protection, access control, logging, audit, and regulatory requirements.	With reference to the data-localization requirements applicable to Offsite Managed Services, including hosting of the Managed Service platform within India, please confirm that the Bank's target systems/data sources configured for inspection and the permitted destinations/integrations for collected data shall also be located in India.	Bank's DC and DR are located in India. Further Detail shall be shared with the successful
1109	56, 257	7.4.3 / 16.21.1 Current IT assets	7.4.3 / 16.21.1	Discovery of internet-facing and internal assets. Servers deployed with OS, DB, Web/app component, middleware's, agents and other applications / software, private & public cloud setups, emerging technologies etc. – 2500; Database – 300; Intranet and internet facing business & non-business applications like CBS, Internet Banking, Mobile Banking, HRMS, O365 etc. – 200; Desktops with various agents like AV, DLP, NAC, ITAM etc. – 12000; Routers & Switches – 7200. Note: The count of IT & Security Infra as listed above is tentative.	Considering the requirement for discovery of internal assets to provide continuous discovery, monitoring, classification, and risk assessment of the Bank's internal attack surface under the ASM Managed Service, please clarify the applicable quantities of servers and desktops to be considered for sizing and licensing, currently indicated in the RFP as 2,500 servers and 12,000 desktops during the contract period.	Bank is lookig for External Attack Surface management, that have been exposed to public
1110	258, 260	16.21.2 Volumetrics-Solution-wise Requirements	16.21.2	XDR (Extended Detection and Response) solution for 12,000 users scalable to 14000 Users' endpoint 12000 scalable to 16000	Considering the user volumetrics specified for XDR and ITDR, please clarify whether 12,000 users, as currently indicated in the RFP, shall be considered for sizing and licensing of the discovery, inventory and monitoring of the Bank's internal attack surface under the ASM Managed Service, including the required scalability during the contract period.	Please refer addendum for revised Volumetrics
1111	169	15.1 Appendix 1A – AI Security	AI Security - 4	Inspect and control prompts, uploads and pastes before data reaches the AI provider.	Customer to accept this capability with delivery within 6 months of go-live, with monitoring and post-submission alerting available from day one.	The Clause reference is not pertaining to this RFP
1112	169	15.1 Appendix 1A – AI Security	AI Security - 5	Allow low-risk activities while blocking upload/paste/share-screen within the same AI app.	Customer to allow this control via integration with the Bank's existing SSE/CASB or endpoint DLP, or accept delivery within 6 months of go-live.	The Clause reference is not pertaining to this RFP
1113	169	15.1 Appendix 1A – AI Security	AI Security - 7	DLP, threat protection and access control in a single inspection pass.	Customer to accept an architecture where AI inspection integrates with the Bank's existing TLS-decrypting proxy/SWG (via ICAP/API), which avoids additional decrypt/re-encrypt cycles without mandating a single engine.	The Clause reference is not pertaining to this RFP
1114	169	15.1 Appendix 1A – AI Security	AI Security - 9	Enforce AI security policy consistently for corporate-managed devices, BYOD and remote/unmanaged endpoints via a cloud-delivered security service edge.	Please clarify whether full policy enforcement is mandatory across all corporate-managed, BYOD and unmanaged/remote endpoint categories from Day 1, and specify the expected SSE deployment model.	The Clause reference is not pertaining to this RFP
1115	169	15.1 Appendix 1A – AI Security	AI Security - 11	The solution must provide granular visibility and control on Generative AI applications (ChatGPT, MS Copilot, etc.), determine the Instance/Tenant being accessed, and enforce dedicated Access Control and Data Protection Policies per Tenant/Instance of the same application.	Specify for which tenant-level identification and dedicated Access Control/Data Protection policies are mandatory.	The Clause reference is not pertaining to this RFP
1116	169	15.1 Appendix 1A – AI Security	AI Security - 17.1	Posture checks: certificate, domain, AV, custom app, process and registry.	Customer to allow device posture signals to be consumed from the Bank's existing EDR/UEM/NAC tools through integration, in place of native posture checks.	The Clause reference is not pertaining to this RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1117	169	15.1 Appendix 1A – AI Security	AI Security - 17.2	The Posture assessment must be periodic in nature and repeat in every 15 minutes or less to ensure continued compliance.	Please confirm whether the 15-minute interval is a strict mandatory maximum, or whether an equivalent event-driven posture re-validation mechanism is also acceptable.	The Clause reference is not pertaining to this RFP
1118	169	15.1 Appendix 1A – AI Guardrails / AI Gateway	AI Guardrails - 9, 10 / AI Gateway - 13, 14	30+ languages and OCR-based inspection of images.	Customer to accept English and Hindi at go-live, with the extended language set and OCR-based image inspection delivered within 6 months of go-live.	The Clause reference is not pertaining to this RFP
1119	169	15.1 Appendix 1A – AI Guardrails	AI Guardrails - 11	Block/allow MCP server code downloads from GitHub based on age, stars, reputation.	Customer to allow it to be met through the Bank's existing SWG/URL filtering combined with the MCP allow-list maintained on the Gateway.	The Clause reference is not pertaining to this RFP
1120	169	15.1 Appendix 1A – AI Guardrails	AI Guardrails - 13	Enterprise DLP integration; CSA-based dynamic risk score; certification reporting.	Customer to retain DLP integration and user coaching, and to accept CSA-based risk scoring and app certification reporting through integration with CASB/third-party feeds, or delivery within 6 months of go-live.	The Clause reference is not pertaining to this RFP
1121	169	15.1 Appendix 1A – AI Gateway	AI Gateway - 1	Provide a centralized AI Gateway that acts as the single inspection and policy-enforcement point for all outbound and internal AI/LLM traffic, including agentic calls.	Please confirm whether 100% of AI/LLM traffic — including direct application-to-provider traffic, agentic traffic, internal LLM traffic and MCP traffic — must mandatorily traverse the AI Gateway.	The Clause reference is not pertaining to this RFP
1122	169	15.1 Appendix 1A – AI Gateway	AI Gateway - 3, 5	Identity-based least-privilege per MCP call; MCP server/tool allow-list and deny-list.	Customer to accept phased delivery: server-level allow/deny list at go-live, with tool-level controls and per-call identity authorization delivered within 6 months of go-live.	The Clause reference is not pertaining to this RFP
1123	169	15.1 Appendix 1A – AI Gateway	AI Gateway - 7	CSA STAR, SOC 2, CIS, ISO 27001/27017/27018 and MAPP membership.	Customer to accept 'or equivalent' certifications, allow certifications held by the hosting data centre/cloud for SaaS components, and remove MAPP as a mandatory criterion for AI security OEMs.	The Clause reference is not pertaining to this RFP
1124	169	15.1 Appendix 1A – AI Gateway	AI Gateway - 9	Software-defined gateway for APIs, internal apps, autonomous agents and private LLMs.	Customer to accept coverage of LLM and agent traffic at go-live, with generic internal API traffic governed via integration with the Bank's existing API gateway.	The Clause reference is not pertaining to this RFP
1125	169	15.1 Appendix 1A – AI Gateway / General	AI Gateway - 10 / General - 1.17	Unified API entry point across LLM providers.	Request the Bank to list the LLM providers and models currently in use and planned (e.g., Azure OpenAI, Bedrock, Vertex AI, self-hosted open models), and the number of internal AI applications to be onboarded behind the gateway.	The Clause reference is not pertaining to this RFP
1126	66, 169	7.6.7 Training / 15.1 Appendix 1A – General	General - 1.20	Bank to create its own semantic detectors without vendor PS.	Please confirm the expected enablement: number of Bank administrators to be trained, and whether a formal training and certification plan is required as part of the deliverables.	Please refer addendum for revised clause
1127	27, 169	7.1 Scope and Objectives / 15.1 Appendix 1A – General	General - 1.27	Native SIEM/SOC integration.	Please confirm the SIEM/SOAR platforms in use, preferred log format and transport (syslog/CEF/API), and expected log volume (EPS).	No Change, Please be guided by the RFP
1128	55, 169	7.4.2 Continuous Automated Red Teaming Services / 15.1 Appendix 1A – General	General - 1.38 to 1.40	Red Team finding mapping, selective re-testing, exportable reports.	Please clarify the red teaming scope: number and type of AI applications, models and agents to be tested, frequency (one-time, quarterly or continuous), and whether the bidder must deliver red-teaming services in addition to platform capability.	Bank is looking for Continuous Automated red teaming services
1129	55, 169	7.4.2 Continuous Automated Red Teaming Services / 15.1 Appendix 1A – General	General - 1.40	Exportable Red Team reports with raw prompts and responses.	Please confirm the Bank accepts redaction of harmful attack payloads in shared reports, with full raw evidence retained in the platform under access control, in line with responsible-disclosure practice.	No Change, Please be guided by the RFP
1130	72–81, 98–99, 140–158	7.12 Resource Requirement; 7.13 Facilities Management; 8 Contract Period; 9 Project Timelines; 13 Service Levels & Penalties	General (Scope)	Implementation and support model.	Request the Bank to confirm the contract period, implementation timeline, on-site FM/resident resource requirement, and the SLA and penalty framework applicable to this solution.	No Change, Please be guided by the RFP
1131			Bid End Date/Time	Bid End Date/Time 30-09-2026	Considering the size of RFP and required technical documentation we request a minimum 2-4 weeks of extension for bid submission timeline.	Please refer addendum for the revised clause
1132			6.16 Bid validity period	The extension of validity period by the Bidder should be unconditional and irrevocable.	The bid validity should be limited to 180 days.	No Change, Please be guided by the RFP
1133			7.1 Scope and Objectives	a. Key Implementation Responsibilities The implementation of each proposed solution, including design, installation, configuration, integration, migration, testing, commissioning, user acceptance testing (UAT), and Go-Live, shall be performed by the respective OEM	Request you to relax this requirement and allow bidder to implement the solutions, OEM can be arranged for validation.	No Change, Please be guided by the RFP
1134			7.2.1 Solutions – Master Deployment Matrix	Network Detection & Response (NDR)	We understand NDR needs to be deployed only at DC & DR location, please share the throughput for sizing.	Please refer addendum for the revised clause
1135			7.2.1 Solutions – Master Deployment Matrix	Deception Technology (Decoy/Honeypot)	What is the number of decoys required ?	Please refer Annexure 21 - Volumetrics- Solution-wise Requirements
1136			7.12.4 Minimum Resource Count Deployment		Please also share the bifurcation of resources across DC & DR location. Can we also provide offsite resources to support the operations ?	No Change, Please be guided by the RFP
1137			7.13 Facilities Management	Bidder should manage, monitor, maintain and upgrade all proposed solutions & services on ongoing basis encompassing all deployed hardware/ firmware/ middleware / software components	Infrastructure management skillset is different from Cyber Security skillset, can we leverage PSB FMS team for managing the VM and below layer ? If not, what is the Infra management resource requirement, can we proposed additional resources for the same ?	The Bidder shall be responsible for managing, monitoring, maintaining, upgrading and supporting all proposed solutions and services, including the deployed hardware, firmware, middleware and software components, as specified in the RFP. The Bidder shall ensure that adequate resources and skillsets are deployed to fulfil all implementation, operation, maintenance, monitoring, troubleshooting and upgrade requirements specified in the RFP. Any additional resources considered necessary by the Bidder to meet its contractual obligations shall be factored into its bid and shall be provided by bidder at no additional cost to the Bank.
1138			7.18.4 Networking and Security Equipment		Can PSB provide racks, cables, switches, routers, load balancers, etc. required for setting up the infra ? Is bidder is expected to provide.	Bank will provide RACK, and TOR Switch. Any Component required for successful installation and implementation shall be factored by the bidder

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1139			10.2 Eligibility Evaluation Criteria		1- Can we involve a distributor for resell of licenses/S/w/ H/w for the solutions? 2 - Can we offer some selected solution in managed service manner where license is always on MSSP name and not transferred to Bank?	No Change, Please be guided by the RFP
1140			10.2 Eligibility Evaluation Criteria	1) The bidder should be an authorized representative/ partner/ reseller of OEM in India. 2) MAF from the respective OEMs of the solution & services	1) Please allow to bidder to be representative of OEM as few of the orders are routed through distributors. 2) Request to edit as "MAF or partnership contract with OEM from the respective OEMs of the solution & services "	No Change, Please be guided by the RFP
1141			10.2 Eligibility Evaluation Criteria	The Bidder must have successfully supplied, installed and maintained (or under maintenance) SIEM Solution of minimum 20000 EPS / 0.86 TB per day in one PSU/ PSE/ Government Organizations / BFSI/Telecom provider in India in last 5 years	Does it also mean resell of licenses ? Or Managed Services will work ?	Please refer the addendum for revised clause
1142			10.2 Eligibility Evaluation Criteria	Bidder should have supplied, installed and maintained (or under maintenance) any three (3) of the below solutions in any one PSU/PSE/ Government Organizations / BFSI in India	Request to make it for any solution and not necessarily for proposed solution.	No Change, Please be guided by the RFP
1143			10.2 Eligibility Evaluation Criteria	The proposed OEM SIEM Solution with a minimum capacity of 30,000 EPS or 1.2 TB/day shall have been successfully implemented and be under management/maintenance in at least one (1) BFSI in India.	1- Request to accept global references as well. 2- Request to you accept on email confirming the credentials without mentioning client name to avoid breach of client NDA. 3- Request you to accept non-BFSI client as well 4- Will only creds where resell of licenses is performed is considered Or Managed Services will work ?	1. No Change, Please be guided by the RFP 2. Client Name & requirement information sought in RFP is mandatory 3. Please refer addendum for revised clause. 4. Please refer addendum for revised clause.
1144			10.3 Technical Evaluation Criteria	Bidder should have supplied, installed and maintained (or under maintenance) from the following solutions:	1- We understood that bidder can give reference of clients with individual solutions and not necessarily single client with all solutions. Pl clarify. 2- Will only creds where resell of licenses is performed is considered Or Managed Services will work ?	1. Experience of solutions can be shown in single /multiple Clients/ work orders meeting the above criteria 2. A bidder's experience in supplying and installing a solution will be considered regardless of when the installation was completed. Even if the installation was completed more than five years ago, it will still qualify, provided the bidder is currently maintaining that solution or has carried out its maintenance at any time during the five-year period preceding the RFP publication date
1145			10.3 Technical Evaluation Criteria	The Bidder must have successfully supplied, implemented, and maintained (or currently be maintaining) a SIEM Solution in at least one PSU/PSE, Government Organisation, BFSI organisation, Telecom provider, with demonstrated deployment experience meeting the following: 1. Point 1: 20000 EPS / 0.86 TB per day ≤ SIEM Solution Experience < 25,000 EPS / 1.00 TB per day 2. Point 2: 25,000 EPS / 1.00 TB per day ≤ SIEM Solution Experience < 30,000 EPS / 1.20 TB per day 3. Point 3: 30,000 EPS / 1.20 TB per day ≤ SIEM Solution Experience	1- Does it mean only proposed SIEM or any other SIEM will qualify for evaluation ? 2- Will only creds where resell of licenses is performed is considered Or Managed Services will work ?	1. Any SIEM solution experience will qualify to demonstrate bidder's experience 2. Bidder's experience in supplying and installing a solution will be considered regardless of when the installation was completed. Even if the installation was completed more than five years ago, it will still qualify, provided the bidder is currently maintaining that solution or has carried out its maintenance at any time during the five-year period preceding the RFP publication date
1146			10.4 Commercial Evaluation Criteria	Award of Contract shall be considered for the bidder ranked L1	Please consider qualifying through QCBS rather than L1.	No Change, Please be guided by the RFP
1147			13.3 At-Risk Amount	The monthly At-Risk Amount (ARA') shall be 15% of the estimated monthly payout of the respective month.	Request to make it 10% of monthly payout	No Change, Please be guided by the RFP
1148			14.1 Assignment & Subcontracting	The selected bidder shall not subcontract/JV/Consortium or permit anyone to perform any of the work, service or other performance required under the contract	Request you to allow subcontract/ consortium	No Change, Please be guided by the RFP
1149			14.13 Indemnity	All indemnities shall survive notwithstanding expiry or termination of Service Level Agreement and the bidder shall continue to be liable under the indemnities	What is the indemnity limit ?	No Change, Please be guided by the RFP
1150				ITSM	What is your current ITSM and ITOM solution used? Can we leverage them? Where is the ITSM deployed? (On-prem, Cloud) Are all the resolver groups of the SOC already configured on the ITSM? As per the RFP - ITSM management will be carried out by NIA and it is outside the scope of the bidder of this RFP? (Is this assumption accurate) Request you to clarify this point in the RFP.	Details shall be shared with succesfull bidder
1151			Annexure 21: Sizing/Volumetrics,	Annexure 21: Sizing/Volumetrics	We understand that there are only two physical data centre sites- DC & DR. Log ingestion will happen only from here. Pl confirm	The bidder shall comply with the locations and architecture specified in the RFP. The bidder shall independently assess all relevant telemetry/data sources, including branches and other specified environments.
1152			Annexure 21: Sizing/Volumetrics,	The bank will procure additional Licenses in the tranches of 10000 EPS/ 420 Gb per day based on the rate provided in the BOM.	Where do we quote in pricing table excel "BOM_PSB SOC RFP" additional rate for each of the solution? It looks missing.	The applicable rate shall be derived on a pro-rata basis from the corresponding rates quoted in the BOM for the respective SIEM Solution.
1153			Annexure 21: Sizing/Volumetrics,	HA (Active/Active – N+N redundant Deployment) at DC and HA (Active/Active – N+N redundant Deployment) at DR	If bidder design management and analytical part in OEM cloud with all SLA/ Uptime compliance, do we need to provide details of HA etc.? Pl clarify that its not required being offered as SaaS.	Please refer addendum for revised clause
1154			7.12.3 Resource Management and Governance	The Bank reserves the right to interview, evaluate, approve, reject, or require replacement of any proposed resource before or during the contract period	As RFP is SLA based with penalty, request to remove this clause and leave it to bidder for best service quality as per RFP	No Change, Please be guided by the RFP
1155				XDR platform should be able to integrate with third party security vendors like Firewall, by ingesting logs for better correlation, in syslog/CEF/LEEF format	Since we are anyways ingesting all the logs in SIEM, request to remove this specifications.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1156				The solution should support Network Behaviour Anomaly detection using full Packet data including L3 / L4 and L7 headers. System should have continuous learning of the traffic baseline and detecting any anomaly for the learned baseline with respect to traffic volume, traffic directionality, protocol usage and unseen application or any specific host / endpoint / user behaving differently	Please let us know how much GB/D traffic you intend to ingest in NDR? Pl clarify that it will be non encrypted and ingested via mirrored port. Please let's know what is the switch mirrored port size and type?	Details shall be shared with succesfull bidder
1157				Product License Cost	Product license cost for Y1 to Y5 is black out. Where should we mention the product license cost?	Reference is not pertaining to this RFP
1158				Entire table	There are few products which may be perpetual and few may be subscription based. We need to know, in this table what should be mentioned? There is no year wise bifurcation mentioned here.	The pricing shall be provided in the two separate sheets provided in the BOM/pricing template: **Product License Cost:** The bidder shall quote the applicable one-time perpetual license cost or initial subscription cost, as applicable, for the respective products/solutions. The relevant product/license details shall be provided in this sheet. **ATS / Annual Subscription Cost:** The bidder shall quote the applicable Annual Technical Support (ATS) / Annual Subscription Renewal Cost in the sheet provided for Y1 to Y5, post Go-Live. The bidder shall clearly identify the applicable licensing model (Perpetual/Subscription) for each product/solution and ensure that there is no duplication between the Product License Cost and ATS/Annual Subscription Cost. The BOM/pricing format remains unchanged.
1159			Functional technical compliance: SOAR	Forensics tools (e.g. FTK, EnCase, Autopsy…)	Please confirm whether the forensics tool support API integration.	No Change, Please be guided by the RFP. Details shall be discussed with successful bidder
1160			Functional technical compliance: SAN Switch	The switch should have non-blocking architecture with all ports active with 32 G SFP+ modules, switch should also support 64G transceiver for future upgrades.	Is bidder required for provide SAN Switch at DC & DR for the SOC infrastructure ? If yes, please clarify the number of switches required. Is bidder expected to provide the RACK, Local callings, etc of Bank will provide it ?	Bank will provide RACK, and TOR Switch. Any Component required for successful installation and implementation shall be factored by the bidder
1161			Functional technical compliance: Load Balancer	The proposed solution should be a dedicated appliance as ADC not as add on license Feature on NGFW and WAF.	Is bidder required for provide Load Balancer at DC & DR for the SOC infrastructure ? Of PSB needs it for their application ? Please explain the requirements along with number of load balancers required.	Bidder to factor the solution/IT Infrastructure component required to ensure the successful implementation of solution keeping in view the deployment requirement, HA (Active-Active) wherever sought
1162			Functional technical compliance: CSP	Data Centres/hosting facilities used by the solution should be minimum Rated 3 of TIA940 or Tier 3 of Uptime Institute or any other equivalent certification	Is this clause applicable for all proposed solution ? If yes, we request you to restrict to SIEM CSP only to ensure solutions meet technical requirements and avoid single vendor lock-in.	Please refer addendum for the revised clause
1163			Functional technical compliance: CSP	Bank will have right to audit the data centre facilities of CSP through any regulators or through any third parties as needed by the regulators and this may entail data localization, sovereignty, confidentiality, and such other things. It's bidder responsibility to enable the same, necessary provision should be incorporated by bidder with CSP to ensure the compliance to the same at no additional cost to Bank.	Many of the solutions/ OEMs host their products on AWS / Azure cloud and offer it to clients. Right to audit to AWS/Azure Data centre will not be allowed as per OEM contracts. Request you to dilute this requirement.	No Change, Please be guided by the RFP
1164				Cloud Security (CSPM) Tool	Please confirm which industry standards/ benchmarks & regulatory compliance should be supported by CSPM tool (Other than ISO 27001, PCI-DSS, NSIT, HIPAA and GDPR mentioned in the RFP)	No Change, Please be guided by the RFP
1165				Cloud Security (CSPM) Tool	Please specify which (Private / Public / Community) cloud environment should be supported by the CSPM Tool	No Change, Please be guided by the RFP, Details shall be shared with the successful bidder
1166				Cloud Security (CSPM) Tool	Please specify the type of automation remediation that should be supported. As CSPM is a detective tool and for automation remediation CWPP would be needed. Please specify features such as CNAPP, CIEM or DSPM should also be supported by the CSPM tool	No Change, Please be guided by the RFP, Details shall be shared with the successful bidder
1167				Cloud Security (CSPM) Tool	Please specify the names of cloud services (IaaS/PaaS) that should be supported by the CSPM Tool	No Change, Please be guided by the RFP, Specific details shall be shared with the successful bidder
1168			Payment Terms-Product (Software) Cost	Milestone based and Quarterly in Arrears	As payment terms mentioned are milestone based and partially as Qarterly in Arrears, requesting the bank to make the payment terms as Annual in Advance.	No Change, Please be guided by the RFP
1169			OEM Services Cost		Our Software and Services go hand-in-hand and should be paid for together.	No Change, Please be guided by the RFP BOM
1170			CSP	Cloud must be hosted in India, and there should be no network and data sharing/replication to any datacenter/office outside the boundaries of India. Bound by Indian law, Indian IT Law, and the applicable regulations. No data in any circumstances should be shared/copied/transmitted without' s consent/written permission of the bank and it should be as per the Indian IT Law, RBI guidelines, bank policy & guidelines and other regulatory & statutory body in India	Our services do not gather any data from the client. We collect data related to the client which is already present on the Surface, deep & dark web. Also, many PSCs, Scheduled Commercial Banks in India are our clients	No Change, Please be guided by the RFP
1171				18 The cloud infrastructure should have presence in at least 2 cities in India in different SEISMIC Zone		Please refer addendum for the revised clause
1172			Penalties-Services SLA	Non-detection or late detection - Rs. 1 Lakh each for non-detection or late detection of phishing site, anti-rogue, malware, social media, mobile app, etc. Point b to Point f -- Rs.5000/- for every hour beyond resolution time.	Requesting the bank to consider better penalty terms, consistent with market standards. These current panalties are very steep. Also, total penlty for a year should be capped at 5% of the yearly contract value.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1173	26	7.1 - Scope and Objectives	7.1	Proposed solutions shall seamlessly integrate with the Bank's existing on-premises, cloud, and hybrid security ecosystem	Please share the OEM/make and model of the Bank's existing core & perimeter network devices - Core Switches, Access/Aggregation Switches, Routers, Load Balancers, and Core/Perimeter Firewalls (NGFW) - at DC, DR and major branches/offices, so bidders can confirm log/telemetry collection compatibility (e.g., syslog, NetFlow/sFlow/IPFIX, SNMP, API) for SIEM, NDR and SOAR integration.	details shall be shared with successful bidder
1174	29	7.2.1 - Solutions - Master Deployment Matrix	7.2.1	For most solutions: 'Bank Location: Broker/Aggregator/Collector: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR' with 'HA Deployment aligned with the SLA, RTO & RPO (Refer Section 13)'	Section 13 (SLA) defines Response Time and Resolution Time by incident severity but does not appear to state explicit numeric RTO (Recovery Time Objective) and RPO (Recovery Point Objective) targets for DC-to-DR failover. Please publish the specific RTO/RPO values (in minutes/hours) applicable to each solution category (SIEM, SOAR, XDR, NDR, etc.) referenced throughout Section 7.2.1, as these directly drive HA/DR architecture and storage replication design.	No Change, Please be guided by the RFP
1175	39	7.3.1.1 - SIEM Modules, Architecture & Deployment	7.3.1.1, Point 4 (and repeated across 7.3.2-7.3.14)	The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution'	Please share the Bank's existing/incumbent MFA/SSO solution (OEM/product name and supported protocols - SAML, OAuth2, RADIUS, etc.) so bidders can confirm integration compatibility for all 14 proposed solutions without needing to propose a generic/unverified integration approach.	The proposed solution shall, by default, provide native Two-Factor Authentication (2FA)/Multi-Factor Authentication (MFA) capability as an integral security feature. The solution shall also be capable of integrating with the Bank's existing MFA solution, if the Bank elects to use the Bank's existing MFA solution for authentication. Where such integration is required by the Bank, the Bank may provide necessary technical details or reasonable support for integration. The Bidder and OEM shall be responsible for ensuring compatibility, configuration and implementation of the required integration as part of their scope.
1176	41	7.3.1.2 - SIEM Data Ingestion & EPS Measurement	7.3.1.2	EPS to be measured at SIEM ingestion boundary; XDR/SIEM data from same OEM must not be double-counted	Please provide a worked numerical example / measurement diagram showing exactly where the EPS meter point sits for a shared-platform SIEM+XDR OEM architecture (i.e., pre-parser vs post-parser, pre-dedup vs post-dedup), so that all bidders size and report EPS on an identical, auditable basis.	No Change, Please be guided by the RFP 7.3.1.2 SIEM Data Ingestion and EPS Measurement
1177	44	7.3.5 - Network Detection and Response (NDR)	7.3.5	NDR shall support integration with the Bank's existing network security environment, SIEM, SOAR, UEBA, XDR, firewall, ITSM	Please confirm whether NDR sensors are expected to be deployed via physical network TAPs, SPAN/mirror ports on existing switches, or virtual TAPs within the Bank's hypervisor/virtualization layer (e.g., VMware/Hyper-V/KVM) for East-West traffic visibility, and identify the Bank's virtualization platform in use at DC/DR.	Please refer addendum for revised clause
1178	45	7.3.7 - Threat Intelligence Platform	7.3.7.1, Point 3	TIP shall aggregate threat intelligence from multiple sources while retaining source/contextual information	Please confirm whether the Bank currently subscribes to any commercial or sector-specific threat intelligence feeds (e.g., IDRBT/CERT-In feeds, ISAC feeds, or existing commercial TI subscriptions) that must be integrated into or migrated onto the new TIP, and share details of any existing feed subscriptions/licenses so their continuity/termination can be planned.	Bidder as a part of holistic solution required to factored in "TIF" i.e commercial as well as OSINT and same is to be integrated with proposed "TIP"
1179	47	7.3.9 - Identity Threat Detection & Response (ITDR)	7.3.9.1, Point 3	ITDR to integrate with Active Directory, LDAP, IAM, PAM, SSO, cloud identity providers	Please confirm the specific IAM/PAM/SSO/Active Directory products currently deployed by the Bank (on-premises and cloud identity providers, if any) so that bidders can validate ITDR integration compatibility and factor in any OEM-specific connector licensing costs.	Please refer the addendum for revised clause
1180	69	7.8 - Non-Functional Requirements	7.8	Non-functional integration, scalability, and interoperability requirements for the proposed solution	Please confirm whether the Bank's existing SOC/ITSM ticketing tool (e.g., ServiceNow or equivalent, referenced generically in Clause 7.13 Point 24) has published REST APIs / webhooks for bidirectional integration with the proposed SOAR platform, and share the ITSM tool's name/version so bidders can validate connector availability.	No Change, Please be guided by the RFP
1181	70	7.9 - Delivery, Installation & Commissioning	7.9	Delivery, Installation & Commissioning requirements for hardware/software across DC, DR and Non-Production sites	Please confirm the exact physical site addresses (DC - Mumbai, DR - Noida, and any additional Non-Production site) along with site-readiness status (power, cooling, rack availability) as of the bid date, to enable accurate installation and logistics planning/costing.	Please refer the addendum for revised clause
1182	72	7.11 - Warranty, ATS and AMC	7.11	Warranty/ATS/AMC applicable to hardware and software; ATS/AMC cost quoted year-wise Y1-Y5 in Commercial BOM	Please specify the standard minimum OEM warranty period (in months, e.g., 12/36) applicable to (a) Hardware/Appliances and (b) Software Licenses supplied under this RFP, so that bidders can correctly determine from which year ATS (software) and AMC (hardware) charges become payable in the Commercial BOM without overlapping the warranty period.	Please refer the addendum for revised clause
1183	75	7.12.4 - Minimum Resource Count Deployment	7.12.4	Minimum onsite L1/L2/L3 resources specified per shift (Shift A: L1-4, L2-2, L3/PM-1; Shift B & C similar); 'bidder to right-size any additional resources' across 16 technology domains plus offsite services	Please confirm whether the stated minimum L1/L2/L3 counts are intended as generalist SOC analyst roles covering all 16 technologies collectively, or whether the Bank expects technology-specialist coverage (e.g., dedicated SIEM/NDR/XDR analysts) in addition to the stated minimums, as this materially affects the FM/O&M resource sizing in the Commercial BOM.	No Change, Please be guided by the RFP
1184	79	7.13 - Facilities Management	7.13, Point 27-28 (General Conditions)	'Integrate the complete proposed setup with all the currently deployed tools and those procured from time to time' and 'integrate...with SIEM, DAM, NBA/NDR, SOAR, TI etc.'	Please provide a consolidated list (OEM/make, model/version) of all 'currently deployed tools' referenced in Clause 27-28 - including existing SIEM (if any), Database Activity Monitoring (DAM), Network Behaviour Anomaly Detection (NBAD), existing SOAR, existing Threat Intelligence feeds, Endpoint AV/EDR, DLP, and NAC solutions currently used by the Bank per the Current IT Assets table (Annexure 21.1) - so bidders can plan connector/API availability and integration effort/cost accurately.	No Change, Please be guided by the RFP
1185	83	7.14 - DR Drill	7.14	DR Drill requirement for the proposed NextGEN SOC solutions	Please specify the mandated minimum frequency of DR drills per year (e.g., half-yearly/quarterly), the maximum permissible downtime/service-impact window during a live DR drill, and whether DR drills must simulate a full DC-to-DR switchover for all 16 solutions simultaneously or can be conducted solution-wise/phase-wise.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1186	89	7.18 - IT Infrastructure Requirements	7.18, Point 3	'The proposed hardware infrastructure should be of the latest production available infrastructure not older than 2025'	Please clarify whether 'not older than 2025' refers to the hardware model's date of General Availability (GA)/announcement, or its date of manufacture, and confirm the applicable cut-off date to be checked - at bid submission, at Purchase Order issuance, or at actual delivery - since delivery may occur several months after PO given the 5-month implementation timeline.	Please refer addendum for revised clause.
1187	89	7.18 - IT Infrastructure Requirements	7.18, Point 17	'Entire solution (hardware & software) should be IPv6 implementation ready from day one'	Please confirm the Bank's current network addressing scheme (IPv4-only, dual-stack, or IPv6) at DC/DR/branches, and specify the exact IPv6-readiness validation/test criteria that will be applied at UAT/Go-Live for the proposed solutions.	Details shall be shared with the successful bidder on a need-to-know basis, as and when required.
1188	89	7.18 - IT Infrastructure Requirements	7.18, Point 1 & GeM Bid Additional Qualification/Data	'Bidder should size hardware based on volumes mentioned in Annexure 21... at relevant locations- DC, DRC and branches'; GeM Bid references a separate 'Network Infrastructure and data flow diagram' document	Please share the existing diagram (showing existing network segments, DMZ, core/aggregation/access switch layers, taps/SPAN points, and firewall zones at DC & DR) as part of the RFP corrigendum so that all bidders can size NDR taps, SIEM collectors and NAC/switch integrations on a common, equal footing.	Details shall be shared with succesfull bidder
1189	90	7.18 - IT Infrastructure Requirements	7.18, Points 9, 19-21	Point 9/21 require production and non-production environments to be 'physically separate'; Point 19 permits 'logical separation/Virtualization' at compute/storage using shared SAN Switch and Backup Solution for both environments	There is an apparent conflict between the mandate for 'physical separation' of production and non-production compute (Points 9, 20, 21) and the provision allowing shared SAN Switch/Backup Solution with only 'logical separation/zoning' (Point 19). Please clarify precisely which infrastructure layers (compute, storage, backup, SAN, network) require physical separation versus which may be logically/virtually separated.	Logical tenancy is acceptable, provided that the proposed bidder/OEM ensure clear separation and isolation of the Bank's data, security telemetry, logs, alerts, configurations, policies, analytics, investigation data and other Bank-related information from those of other tenants. The proposed environment for bank are protected against confidentiality and integrity risks and co-mingling of data and bidder/OEM implement adequate safeguards against combining of information, documents, records and assets.
1190	91	7.18.1 - Compute Infrastructure	7.18.1, Point 12	'Bidder is required to factor in the necessary compute resources for analytics, AI/ML modeling, etc.' and GPU line item present in Commercial BOM Hardware Cost sheet	Please specify the intended AI/ML/NLP/Analytics use case(s) the Bank expects the proposed SOC solutions to support (e.g., LLM-based alert summarization, anomaly-detection model training, local vs. cloud-hosted AI/ML), and provide indicative GPU compute sizing guidance (GPU type/count) so bidders can size the 'GPUs' line item in the Hardware Cost BOM sheet consistently.	The Bidder/OEM to right size and factors in the compute resources necessary to deliver the AI/ML, analytics, automation, anomaly detection, threat detection, correlation and other analytical capabilities proposed as part of the solution. The Bidder/OEM shall therefore determine and propose the appropriate compute/GPU sizing based on the architecture, deployment model, solution capabilities, workload, data volumes and performance requirements of the proposed solutions. Where AI/ML capabilities are provided through the OEM's SaaS/cloud service or OEM-managed infrastructure, the corresponding underlying GPU/compute infrastructure needs to be factored by bidder/OEM ensuring SLA compliance
1191	92	7.18.2 - Storage Infrastructure - Primary (SAN Switch dependency)	7.18.2 & Commercial BOM (Hardware Cost - SAN Switches line item)	Commercial BOM Hardware Cost sheet includes a 'SAN Switches' line item with a note: 'Bank will provide the Ports on their LEAF and OOB switches. Bidder is required to explicitly provide the port requirements on LEAF and OOB switches'	Please confirm the existing SAN fabric switch OEM/model, available Fibre Channel (FC) port count/speed (8G/16G/32G) at DC & DR, and whether bidders should quote new dedicated SAN switches in the BOM or can assume connectivity to the Bank's existing SAN fabric with adequate free ports for the proposed storage.	Bank will provide RACK, and TOR Switch. Any Component required for successful installation and implementation shall be factored by the bidder
1192	93	7.18.4 - Networking and Security Equipment	7.18.4	Bidder to propose networking and security equipment required for the solution deployment	Please confirm the number of physical network ports (LEAF/TOR/OOB switch ports) and rack units the Bank will make available for bidder-supplied appliances at each of DC-Primary, DC-HA, DR-Primary, DR-HA and Non-Production environments, since this is referenced as a Bank-provided dependency in the Commercial BOM notes (SAN Switch sheet) but not quantified elsewhere in the RFP.	details shall be shared with successful bidder
1193	93	7.18 - IT Infrastructure Requirements	7.18, Point 13 & 7.18.4	'Bidder shall be responsible for providing all the logs and required telemetry data for the setup and ensuring its integration with the centralized SOC of PSB'; networking/security equipment references LEAF and OOB switches	Please confirm whether the Bank's existing LEAF/OOB/TOR switches (referenced in the Commercial BOM's SAN Switch notes) support port mirroring/SPAN or a network TAP infrastructure suitable for NDR/IDS sensor placement, or whether the bidder is expected to supply dedicated TAP aggregators; also confirm available spare ports on existing switches versus ports the bidder must provision.	Bank will only provide the connectivity and ports on the Core Switch supporting 10/25 G Ports.. Anything else required for the implementation should be factored in by the Bidder.
1194	93	7.19.3 - Security Management / 7.18 IT Infrastructure (Patch Management)	7.19.3 & 13.1 (SLA - Version Upgrades, Security Patching)	'Bidder onsite personnel should be carrying out regular patch management...of the deployed solution' (Cl. 7.13 Pt.5) and SLA Cl. 13.1 mandates 95% monthly patch-compliance for 'OS, database, middleware, application, firmware' patches - no dedicated 'Patch Management' tool appears in the 14-solution list or Commercial BOM	Please confirm whether the Bank has an existing centralized Patch/Vulnerability Management tool (e.g., SCCM/WSUS/ManageEngine Patch Manager Plus/BigFix or similar) that the bidder is expected to use/integrate with for OS, firmware and middleware patching of the newly supplied NextGEN SOC servers/appliances, OR whether the bidder must independently procure and operate its own patch management solution/process (in which case, please confirm whether this should be a separately licensed tool or a manual/scripted process covered under FM services) since 'Patch Management' is not listed as a distinct line item anywhere in the Commercial BOM.	Bank has ITSM Solution (Manage Engine)
1195	93	7.19.3 - Security Management (Patch Testing)	7.19.3	Patch/upgrade implementation is measured under SLA (95% MSL) but the RFP does not specify a mandatory patch validation/staging step	Please confirm whether all OEM-released patches/updates must first be validated in the Non-Production environment before production deployment, and specify the maximum permissible time window between patch release (or OEM critical-severity advisory) and mandatory production implementation, to align with the Bank's Change Management and patch SLA (Section 13.1) requirements.	No Change, Please be guided by the RFP
1196	93	7.18.4 - Networking and Security Equipment (Existing Switch Port Availability)	7.18.4	Bidder to propose networking and security equipment required for solution deployment; no port/capacity details of existing switching infrastructure are provided	Please share the existing LEAF, OOB, TOR/Access and Core Switch port availability (spare port count by speed - 1G/10G/25G/40G/100G, and interface type - Copper/SFP+/QSFP) at each of DC-Primary, DC-HA, DR-Primary and DR-HA, so that bidders can size their appliance NICs, uplinks, and any additional switching hardware they may need to propose in the Commercial BOM accordingly, rather than assuming unlimited free ports on Bank-owned switches.	details shall be shared with successful bidder

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1197	93	7.18.4 - Networking and Security Equipment (Switch Make/Model & Protocols)	7.18.4	Bank will provide the Ports on their LEAF and OOB switches; Bidder to explicitly state port requirements (per Commercial BOM SAN Switch sheet notes)	Please share the OEM/make and model of the existing LEAF and OOB switches, and confirm supported switching features required for appliance connectivity - LACP/Port-Channel bonding, 802.1Q VLAN trunking, Jumbo Frame (MTU 9000) support, and Spanning-Tree mode - so bidders can design NIC teaming and network segmentation for the proposed SIEM/NDR/XDR/Decoy appliances consistent with the Bank's existing switch configuration.	No Change, Please be guided by the RFP . Refer Section 13 - SLA & Penalty
1198	94	7.19.2 - Transition Management	7.19.2, Points 1-4	Bank to provide existing security infrastructure details and OEM support contracts at project initiation; Bidder to run existing SIEM 'as-is/where-is' for 12 months from Go-Live, effective 01.05.2027	Please name the current SIEM OEM/platform and the incumbent service provider (or confirm if this will be disclosed only to the successful bidder post-award), and clarify whether the new NextGEN SIEM must run in parallel with the existing SIEM for the full 12-month transition period (dual-run), or whether the 12-month 'as-is/where-is' obligation applies only if the new SIEM's Go-Live is delayed beyond 01.05.2027.	The existing SIEM/SOC platform is operational and will be replaced under this RFP. No data migration from the existing SIEM/SOC is envisaged. The existing platform shall run in parallel with the proposed solution for a limited period to meet compliance requirements. The Bidder shall not require to factor any existing OEM Services cost for such parallel operation period, support is to be provided on best effort basis. The Bidder shall ensure successful Go-Live of the proposed solution within the prescribed implementation timeline, irrespective of the parallel operation of the existing SIEM/SOC.
1199	95	7.19.3 - Security Management	7.19.3	Security Management requirements for the proposed NextGEN SOC solutions and infrastructure	Please clarify whether periodic VAPT (Vulnerability Assessment & Penetration Testing) of the bidder-supplied NextGEN SOC infrastructure itself (as distinct from the VA-VM tool the bidder is deploying for the Bank's IT assets) is in scope of the bidder's responsibility, and if so, the expected frequency (e.g., annual/half-yearly) and whether it is to be performed by the bidder or a Bank-appointed third party.	Periodic Vulnerability Assessment and Penetration Testing (VAPT) of the bidder/OEM-supplied NextGEN SOC solution and its deployed infrastructure/components shall be within the scope of the Bidder/OEM The VAPT requirement for the NextGEN SOC infrastructure is distinct from the VA/VM solution being procured for assessment of the Bank's IT assets. For OEM-hosted SaaS services, the OEM shall provide relevant assessment reports/certifications or appropriate evidence to the Bank. The Bidder/OEM shall be responsible for remediation of vulnerabilities attributable to its supplied solution/components within the timelines prescribed by the Bank/RFP and shall provide appropriate remediation evidence or closure reports.
1200	95	7.19.3 - Security Management	7.19.3	Integration with authentication/authorization mechanisms enforcing the Bank's security policies	Please confirm the Bank's existing Identity & Access Management stack - Active Directory/LDAP, IAM, Privileged Access Management (PAM/PIM), and SSO/MFA solution (OEM/product name) - so bidders can validate out-of-the-box connector availability for SIEM, SOAR, UEBA and ITDR rather than relying on custom integration.	Details shall be shared with the successful bidder
1201	101	10.2 Eligibility Evaluation Criteria Sr. no 6	Sr. no 6	The bidder should have a minimum average turnover of INR 500 crore per annum in India during the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth.	We request you to amend the clasue as; The bidder should have a minimum average turnover of INR 300 crore in India during the past 3 financial years (i.e. 2023-24, 2024-25 and 2025-26) along with positive net worth.	No Change, Please be guided by the RFP
1202	103	10.2 Eligibility Evaluation Criteria Sr. no 7	Sr. no 7	The Bidder must have successfully supplied, installed and maintained (or under maintenance) SIEM Solution of minimum 20000 EPS / 0.86 TB per day in one PSU/ PSE/ Government Organizations / BFSI/Telecom provider in India in last 5 years	We request you to amend the clasue as; The Bidder must have successfully supplied, installed and maintained (or under maintenance) SIEM Solution of minimum 2,000 EPS in one PSU/ PSE/ Government Organizations / BFSI/Telecom provider in India in last 5 years	Please refer addendum for revised clause.
1203	105, 106	10.3 Technical Evaluation Criteria Bidder's Scoring Criteria Sr. No. 8	Sr. No. 8	Bidder should have supplied, installed and maintained (or under maintenance) the below solutions in any one PSU/PSE/ Government Organizations / BFSI /Telecom provider in India 1. SOAR 2. UEBA 3. Extended Detection & response (XDR)/ Endpoint Detection & response (EDR) 4. Network Detection & response (NDR) 5. Threat Intelligence Platform 6. Vulnerability Assessment / Vulnerability Management 7. Identity Threat Detection & response (ITDR) 8. Decoy/Honeypot/Deception 9. Application security testing tool (DAST/SAST) 10. CSPM Scoring: Point 1: Experience in 3 solutions – 8 Marks Point 2: Experience in 4 solutions –10 Marks Point 3: Experience in 5 solutions –12 Marks Point 4: Experience in more than 5 solutions– 15 Marks	We Request you to amend the scoring as; Scoring: Point 1: Experience in 3 solutions – 8 Marks Point 2: Experience in 4 solutions –10 Marks Point 3: Experience in 5 or more than 5 solutions –15 Marks	Please refer addendum for the revised clause
1204	130	10.3 Technical Evaluation Criteria Bidder's Scoring Criteria Sr. No. 2	Sr. No. 2	The Bidder must have successfully supplied, implemented, and maintained (or currently be maintaining) a SIEM Solution in at least one PSU/PSE, Government Organisation, BFSI organisation, Telecom provider, with demonstrated deployment experience meeting the following: 1. Point 1: 20000 EPS / 0.86 TB per day ≤ SIEM Solution Experience < 25,000 EPS / 1.00 TB per day 2. Point 2: 25,000 EPS / 1.00 TB per day ≤ SIEM Solution Experience < 30,000 EPS / 1.20 TB per day 3. Point 3: 30,000 EPS / 1.20 TB per day ≤ SIEM Solution Experience	We request you to amend the clause as; The Bidder must have successfully supplied, implemented, and maintained (or currently be maintaining) a SIEM Solution in at least one PSU/PSE, Government Organisation, BFSI organisation, Telecom provider, with demonstrated deployment experience meeting the following: 1. Point 1: 2,000 EPS per day ≤ SIEM Solution Experience < 25,00 EPS 2. Point 2: 2,500 EPS ≤ SIEM Solution Experience < 3,000 EPS 3. Point 3: = 3,000 or more EPS	Please refer addendum for revised clause.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1205	126	10.3 - Technical Evaluation Criteria (Note)	10.3 Note (Page 126)	'In the event a Bidder participates in both the NextGen SOC RFP and IT Security solution (Part A/Part B and Firewall) & services RFP...' indicates Firewalls are being procured under a separate, concurrent RFP	Please confirm (a) whether the Bank's Firewalls (Perimeter/Core NGFW) are existing/legacy devices to be integrated as-is, or new firewalls being procured under the separate 'IT Security Solution (Part A/Part B and Firewall)' RFP running in parallel; (b) the expected award/go-live timeline of that Firewall RFP relative to this NextGEN SOC RFP's 5-month implementation window; and (c) which OEM/firewall platform NDR, SOAR and SIEM must integrate with at Go-Live.	The Bank is undertaking new procurement and implementation of multiple IT security components through separate and concurrent procurement processes, including the Firewall/IT Security Solution procurement. The Bank may deploy new Firewall/NGFW/IT security infrastructure under the separate procurement, and the selected NextGEN SOC Bidder shall be required to perform integration with the Firewall/NGFW/IT security solution(s) deployed by the Bank. Bidder/OEM proposed solution shall be capable of integrating with the Firewall/NGFW/IT security solution(s) deployed under the Bank's security architecture, and the Bidder/OEM shall provide the required integration, configuration and correlation capabilities within the scope of the RFP. The Bidder shall factor the necessary integration/re-integration effort, APIs, connectors, configuration, testing and coordination with the relevant OEM/solution provider
1206	140	13 - Service Levels & Penalties	13.1	SLA defines Response Time (15 min) and Resolution Time (45/90/150 min) by severity, but no explicit system/solution-level Availability % (uptime) target (e.g., 99.9%) is stated for individual solutions	Please specify the minimum guaranteed Availability/Uptime percentage (e.g., 99.9%, 99.95%) applicable to each in-scope solution (SIEM, SOAR, NDR, etc.) and to the underlying IT infrastructure (compute/storage/network), as 'uptime' is referenced in Clause 13.1(4)/(12) for penalty calculation but no target percentage is specified.	No Change, Please be guided by the RFP
1207	169	Appendix 1A - Functional Compliance Sheet (Solutions)	Appendix 1A, Summary Tab	Solution list S.No. column: ITDR and CSPM both numbered '9'; sequence jumps from 12 (CWPP) directly to 14 (CTEM), skipping 13	The Summary tab of Appendix 1A (Functional Compliance Sheet - Solutions) has duplicate and skipped serial numbers (ITDR & CSPM both listed as Sl. No. 9; Sl. No. 13 is missing between CWPP and CTEM). Please issue a corrected Appendix 1A with unique, sequential serial numbers for all 14 solutions, and confirm the Maximum Marks weightage assigned to each individual solution sheet, since only the Grand Total (100 marks) is currently visible in the summary.	No Change, Please be guided by the RFP
1208	169	GeM Bid - Additional Qualification/Data Required	GeM Bid Document, Additional Doc References	GeM Bid references separate attachments: 'Network Infrastructure and data flow diagram', 'Scope of Work', 'Format of NDA', and 'Format for breakup of components on cost/price offered' as uploaded PDF documents	Please confirm that the RFP document (273 pages) and its Appendices/Annexures are the single source of truth for technical scope, and that the separately uploaded GeM PDF attachments (Network Infrastructure/data flow diagram, SOW, NDA format) are fully consistent with and do not introduce any additional/conflicting technical requirement beyond what is stated in the main RFP body.	Yes, the Document published are single source of truth (RFP, Appendix, Annexures) . Please refer addendum for the revised Clauses
1209	256	16.21 - Annexure 21, Volumetrics table (numbering)	16.21.2	Solution-wise Volumetrics table Sl. No. sequence reads: 1 (Non-Production), 1 (SIEM - unnumbered restart), 4 (SOAR), 5 (XDR), 6 (NDR), 7 (UEBA), 8 (Decoy)... - Sl. No. 2 and 3 are missing	The Volumetrics table in Annexure 21 has a numbering discontinuity (Sl. No. 2 and 3 do not appear before Sl. No. 4 - SOAR). Please republish a corrected Annexure 21 with consistent serial numbering covering every proposed solution, to avoid any ambiguity on whether a solution's volumetrics were inadvertently omitted.	Please refer addendum for the revised clause
1210	257	16.21.1 - Current IT Assets (Branches)	16.21.1	'Desktops with various agents like AV, DLP, NAC, ITAM etc. - 12,000' and 'Routers & Switches - 7,200'	Please confirm the OEM(s) of the existing endpoint Antivirus/EDR, DLP, and NAC agents deployed on the 12,000 desktops, and the OEM(s)/models of the 7,200 branch routers & switches, so bidders can confirm whether existing agents can dual-forward logs to the new SIEM/XDR without requiring re-agent deployment, and whether branch network devices support remote syslog/NetFlow export for centralized SOC visibility.	The Bank has already provided the relevant volumetrics and sizing parameters in the RFP/SRS. The Bidder shall accordingly size and propose the solution to ensure compliance with all specified functional, technical, performance, capacity and SLA requirements. Details of the Bank's existing infrastructure, environment, configurations and other relevant technical information required for detailed implementation and integration shall be shared with the successful bidder during the implementation phase, subject to the Bank's applicable security and information-sharing policies.
1211	258	16.21.2 - Annexure 21, Volumetrics (SIEM)	16.21.2, Sl. No. 1 (SIEM)	Total 50,000 sustainable EPS/2.06 TB per day scalable to 75,000 EPS/3.09 TB per day at DC & DR; each node/environment individually provisioned for full peak load	Please confirm whether 50,000/75,000 EPS is the aggregate ingestion across DC+DR combined, or whether each of DC and DR must independently sustain the full 50,000/75,000 EPS (i.e., 100,000/150,000 EPS combined capacity), given the note that 'each node/environment must be individually provisioned for full peak load'.	Please refer the addendum for revised clause
1212	258	16.21.2 - Annexure 21, Volumetrics (UEBA)	16.21.2, Sl. No. 7 (UEBA)	UEBA volumetrics stated as identical to SIEM: Total 50,000 EPS/2.06 TB per day scalable to 75,000 EPS/3.09 TB per day	Please clarify whether UEBA is expected to independently ingest and store the same 50,000-75,000 EPS of raw log data as SIEM, or whether UEBA is expected to consume normalized/enriched events from the SIEM data platform (shared ingestion). This materially changes UEBA compute/storage sizing.	Please refer the addendum for revised clause
1213	259	16.21.2 - Annexure 21, Volumetrics (XDR)	16.21.2, Sl. No. 5 (XDR) vs. 10.2 & 7.3.14 (ITDR/CTEM)	XDR volumetrics state '12,000 users scalable to 14,000'; ITDR and CTEM volumetrics elsewhere state '12,000 users scalable to 16,000'	There is an inconsistency in the maximum scale-up user count between XDR (14,000) and ITDR/CTEM (16,000). Please confirm the correct target endpoint/user scale-up figure to be used uniformly for XDR, ITDR and CTEM sizing and licensing.	Please refer addendum for the revised clause
1214	259	16.21.2 - Annexure 21, Volumetrics (Decoy)	16.21.2, Sl. No. 8 (Decoy/Honeypot)	Solution must cover minimum 200 applications, networks, devices with 50 segments across DC-DR	Please define 'segment' in this context (VLAN, subnet, or network zone) and confirm whether the 50 segments and 200 applications/networks/devices are to be deployed only at DC & DR, or also extend to select branch/regional network segments.	Please refer the addendum for revised clause
1215	259	16.21.2 - Annexure 21, Volumetrics (NDR)	16.21.2, Sl. No. 6 (NDR)	Throughput requirement of 10 Gbps	Please confirm whether the 10 Gbps throughput requirement applies per monitored network segment/tap point, or as an aggregate across all DC/DR network taps/SPAN/mirror ports, and indicate the expected number of tap/SPAN points at DC and DR for NDR sensor sizing.	Please refer addendum for revised clause
1216	259	16.21.2 - Annexure 21, Volumetrics (AST)	16.21.2, Sl. No. 12 (Application Security Testing)	SAST - 1 Enterprise License (unlimited apps/scans, 30 users); DAST - 1 Enterprise license for min. 25 web-facing applications; no separate mobile app count stated	Section 7.3.10 states the Bank intends to test Web Applications, Mobile Applications & APIs. Please provide the expected number of Mobile Applications and APIs to be onboarded for security testing, as the current volumetrics table only specifies counts for Web (DAST) applications.	details shall be shared with successful bidder

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1217	260	16.21.2 - Annexure 21, Volumetrics (CSPM)	16.21.2, Sl. No. 13 (CSPM)	'At least 20 VMs (VPCs)'	The unit of measure 'VMs (VPCs)' appears to conflate two different constructs. Please clarify whether the sizing basis is 20 Virtual Private Clouds/Virtual Networks, or 20 Virtual Machines, and separately confirm the number of Cloud Service Provider accounts/subscriptions (AWS/Azure/GCP/OCI) to be covered.	No Change, Please be guided by the RFP
1218	260	16.21.2 - Annexure 21, Volumetrics (CNAPP/CWPP)	16.21.2, Sl. No. 14 & 15 (CNAPP, CWPP)	20 VPCs/Vnets and VM Count of 100 for both CNAPP and CWPP	Please confirm whether CNAPP and CWPP are sized for the same 20 VPCs/Vnets and 100 VMs (i.e., overlapping scope covered by two different tool categories), and provide the expected number of Kubernetes clusters/nodes, containers, and serverless functions to be protected, as these are called out functionally in Sections 7.3.12/7.3.13 but not quantified in the volumetrics table.	No Change, Please be guided by the RFP
1219	260	16.21.2 - Annexure 21, Volumetrics (CTEM vs VA-VM)	16.21.2, Sl. No. 10 (VA-VM) & 16 (CTEM)	VA-VM sized for 'Minimum 4,000 IPs'; CTEM states 'Vulnerability/Exposure findings - Unlimited' and 'IPs - 4,000'	Please clarify whether the CTEM tool is expected to consume vulnerability data from the same standalone VA-VM tool (integration only), or whether CTEM requires its own independent vulnerability-scanning engine/license in addition to the separately-quoted VA-VM tool, to avoid ambiguity in the Commercial BOM licensing structure.	No Change, Please be guided by the RFP
1220	261	16.21.3 - Deployment and Data Retention	16.21.3	Retention table specifies Daily Incremental Backup (2 weeks), Weekly Full Backup (2 weeks), Monthly Full Backup (2 months), and 'Duration of the Contract' for Long-Term Storage (LTS)	Please clarify separately the required Hot/Warm (searchable & query-able online) retention period versus Cold/Archived (LTS, restorable on request) retention period specifically for SIEM raw logs and correlated events, since this is the single largest driver of primary storage sizing and is not explicitly split out in the current retention table.	Please refer addendum for revised clause
1221	261	16.21.3 - Deployment and Data Retention (Log Retention)	16.21.3	Backup retention table covers Daily Incremental (2 weeks), Weekly Full (2 weeks), Monthly Full (2 months), LTS (Entire Duration of Contract) - this appears to describe backup-copy retention, not SIEM's native online log retention	Please confirm the mandatory Online/Hot (searchable within the SIEM console without restoration) log retention period separately from the Backup/Archival retention period specified in Annexure 21, in line with RBI/CERT-In log retention guidance (e.g., minimum online retention of 90/180/365 days), as this is the primary driver of SIEM primary storage (hot-tier) sizing and is currently undefined.	Please refer addendum for revised clause
1222	261	16.21.3 - Deployment and Data Retention (Backup Policy Reference)	16.21.3 & 7.18.3, Point 2	'Bidder to factor the required solution and infrastructure to ensure taking and securing backup as per the PSB policy (which will be updated from time to time)'	Please share the Bank's current Backup & Data Retention Policy document (or its key parameters - backup frequency, RPO for backup jobs, encryption-at-rest requirement, immutability/ransomware-protection requirement) referenced in Clause 7.18.3, since bidders are required to size Backup Software, Backup Server and Long-Term Storage strictly 'as per the PSB policy' without visibility into that policy.	details shall be shared with successful bidder
1223	261	16.21.3 - Deployment and Data Retention (Sizing Assumptions)	16.21.3	Backup/LTS sizing to consider 'deduplication and/or compression efficiency (where applicable)'	Please confirm whether the Bank has a target/expected deduplication and compression ratio to be assumed for Backup and Long-Term Storage sizing (e.g., 2:1, 4:1), or whether bidders should size on a 1:1 (no dedupe/compression credit) basis for evaluation-parity across bidders using different backup OEMs.	No Change, Please be guided by the RFP. Bidde rto design the solution
1224	Appendix 1A	Functional Compliance Sheet - XDR, Clause 50	Bidders must propose a solution which is easy-to-manage, clientless platform that gets deployed quickly and involves minimal or no dependency on customization and management of operating environment.	XDR platform deployment model	Kindly clarify whether the proposed XDR component is intended to be agent-based (as implied by Clause 8, which references agent version control) or clientless/agentless (as stated in Clauses 51/53). If a combination is acceptable (e.g., agent-based endpoint detection along with agentless network-level telemetry), kindly confirm this is permitted and how compliance should be evidenced.	No Change, Please be guided by the RFP
1225	Appendix 1A	Functional Compliance Sheet - XDR, Clause 51	Easy-to-manage, clientless platform that deploys quickly and involves minimal or no dependency on customization and management.	XDR platform deployment model		No Change, Please be guided by the RFP
1226	Appendix 1A	Functional Compliance Sheet - XDR, Clause 51	Easy-to-manage, clientless platform that deploys quickly and involves minimal or no dependency on customization and management.	XDR platform deployment model		No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1227	2	Appendix-1B_TRS	Primary Storage	Proposed storage solution should be offerred with minimum 2 controllers with minimum 256 GB DRAM Cache memory on the entire storage Solution. The solution should scale to atleast 512GB Cache memory by adding additional controller. The proposed array must protect data in cache during a manual power down or an unexpected power outage by vaulting to flash storage. The NVMe SSD capacity drives must not be used for any caching requirements of the storage. The caching requirements of storage must be factored separately	Bidder Request to change the clause to "Proposed storage solution should be offerred with minimum 2 controllers with minimum 512GB DRAM Cache memory on the entire storage array on day1. The proposed array must protect data in cache during a manual power down or an unexpected power outage by vaulting to flash storage or better. Reason for change: - 256GB Total Memory which is 128GB Per Controller is too less and hence request to include Total of 512GB (256GB Per controller) from Day1 itself. - Secondly, New Generation NVMe based array whcih are builtup from ground to harness the full benefits of Very high parallel processing of NVMe uses diffent architecture. The current clause is restrictive hence request to change.	No Change, Please be guided by the RFP
1228	2	Appendix-1B_TRS	Primary Storage	The proposed array should be configured with at least 8 x 32Gbps & 8 x 10Gbps optical front-end ports & Proposed storage should support 100GbE backend.	The proposed array should be configured with at least 8 x 32Gbps & 4 x 10/25Gbps optical front-end ports & Proposed storage should support 100GbE backend. Reason for Change: 8 Number of ethernet ports for front-end connectivity is not appropriate as the FC ports are already asked for Host Connectivity. We request to please reduce the ethernet ports to avoid vendor lock-in as current clause is restrictive.	Please refer the addendum for revised clause
1229	2	Appendix-1B_TRS	Primary Storage	The proposed array must support the latest industry standard (No proprietary) dual ported NVMe TLC / QLC drives.	Please confirm if TLC drives should be provided or QLC. Please Note- TLC Drives are for high performance low latency workloads like OLTP, Virtualization, Databases etc. whereas QLC drives are more appropriate for Data Archival, Backups, Non-Latecny sensitiv workloads etc.	No Change, Please be guided by the RFP
1230	3	Appendix-1B_TRS	Primary Storage	The proposed array should be proposed with native IP ports for remote replication to DR site with appropriate licenses. If separate FCIP routers are required for replication, then the same should be included in the BOM (Min 2 Nos per site). Proposed storage system should be capable of native storage based asynchronous replication.	We suggest to include Native storage based Sync Replication also for Zero Data Loss support and to avoid any additional cost. Secondly, please confirm if Bank is looking for Near-zero (<1 minute) RPO support for Long Disktance Async Replication on the storage?	No Change, Please be guided by the RFP
1231	3	Appendix-1B_TRS	Primary Storage	The proposed Storage solution should support or integrate with software (either OEMprovided or third-party) capable of automating and orchestrating application/database-consistent copies for applications including, but not limited to, MSSQL, Oracle, Exchange, to support use cases such as data repurposing, off-host backup, Test/Dev, Reporting, etc.	The mentioned feature is applicable for Bacup software solution hence request to change the clause to "The proposed Storage/Backup solution should support or integrate with software (either OEMprovided or third-party) capable of automating and orchestrating application/database-consistent copies for applications including, but not limited to, MSSQL, Oracle, Exchange, to support use cases such as data repurposing, off-host backup, Test/Dev, Reporting, etc."	No Change, Please be guided by the RFP
1232	3	Appendix-1B_TRS	Primary Storage	The proposed array must include SED (or hardware) based data at rest encryption solution to encrypt data on all drives (AES 256 bit) with embedded automated key management. Encryption should seamlessly work with all the storage features and without any performance penalty.	Today there are real thret of ransomeware and cyber resilence Storage is one of the key requirement for almost every enterprise and for it is even more importtant fincial services and banking customers hence For Data Security and protection we suggest to please include additional clause as "Offered Storage should be provided with Randsomeware Detection and Protection both for the entire proposed capacity and array if the capability is not native on the storage bidder is free to provide solution with required software and hardware in redundant configuration. additionally offered each Storage controller shall have redundant secure encrypted NVMe Boot Drive for security and protection.	No Change, Please be guided by the RFP
1233	7	Appendix-1B_TRS	Backup Solution	Should be able to archive ALL workloads (VMs, DBs, Files) backup data by moving it to another disk target with different hardware using NFS/S3 protocols for long term retention and all the licenses for backup software and backup storage must be provided on day 1.	Current clause is restricting the backup target to be only NAS or S3 only. Hence request to please change the clause to "Should be able to archive ALL workloads (VMs, DBs, Files) backup data by moving it to another disk target with different hardware using NAS/S3/Catalyst/SAN protocols for long term retention and all the licenses for backup software and backup storage must be provided on day 1."	Please refer the addendum for revised clause
1234	7	Appendix-1B_TRS	Backup Solution	The proposed backup solution must support provide Data protection, Replication, Encryption, Immutability, MFA (Multi-factor authentication) and archival to external NFS/S3 based storage from day 1 and all these licenses must be included.	Current clause is restricting the backup target to be only NAS or S3 only. Hence request to please change the clause to "The proposed backup solution must support provide Data protection, Replication, Encryption, Immutability, MFA (Multi-factor authentication) and archival to external NAS/S3/Catalyst/SAN based storage from day 1 and all these licenses must be included."	Please refer the addendum for revised clause
1235	9	Appendix-1B_TRS	Backup Solution	The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data over a secure, API-based disk-to- disk (D2D) connection.	Request to change the clause to "The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data over a secure, API-based disk-to- disk (D2D) connection. The proposed disk-based storage/appliance shall be certified to work with at-least 3 Backup application vendor ISVs like Commvault, Veeam and Cohesity etc." Reason for change: The requested change will ensure that your investment is protected by allowing to integrate with leading enterprise backup softwares and not just with only one backup software. The Backup Storage Applinace should be certified to work with multiple Backup Software ISVs and not restricted to single Backup software which will allow customer the flexibility of choice of backup software and investment protection.	Please refer the addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1236	9	Appendix-1B_TRS	Backup Solution	Proposed Disk Based Appliance/backup storage should have the capability to tier backup data to an external cloud storage (on premise / public cloud) and the required licenses must be provided on day 1. Proposed backup solution with storage/appliance should have redundant components (Backup Storage - controllers, Power, fans etc. and Backup Appliance - Power, fans etc.), HA mechanism in place to avoid Single Point of Failure and should have minimum of 4x16/32 GB FC ports & 2x32G ports on each controller for Host connectivity. Proposed Backup Solution should have minimum 4x scalability of the current quoted capacity for future growth.	Proposed Disk Based Appliance/backup storage/Backup Solution should have the capability to tier/Move backup data to an external cloud storage (on premise / public cloud). Proposed backup solution with storage/appliance should have redundant components (Backup Storage - controllers, Power, fans etc. and Backup Appliance - Power, fans etc.), HA mechanism in place to avoid Single Point of Failure and should have minimum of 4x16/32 GB FC ports OR 2x32G ports on each controller for Host connectivity. Proposed Backup Solution should have minimum 4x scalability of the current quoted capacity for future growth. Reason for change: Current clause is restrictive as the asked functionality is not completely at storage/appliance level but is applicable at Backup Solution level and hence request to please change.	Please refer addendum for revised clause
1237	10	Appendix-1B_TRS	Backup Solution	The proposed appliance/backup storage must ensure that all scheduled backups complete within an 8-hour backup window, with data protected via RAID 6 (or equivalent - providing 2 disk failure protection). Backup solution must support required technology and storage capacity to manage and compensate duplication across multiple pools, ensuring consistent performance and efficiency. Overheads in terms of memory, capacity, technology and IOPS to handle the bottleneck due to multiple deduplication pools should be factored and required documentation from the OEM is to be submitted along with the proposal.	The proposed appliance/backup storage must ensure that all scheduled backups complete within an 8-hour backup window, with data protected via RAID 6 (or equivalent - providing 2 disk failure protection). Backup solution must support required technology and storage capacity to manage and compensate duplication across/within multiple pools, ensuring consistent performance and efficiency. Backup storage Overheads in terms of memory, capacity, technology and IOPS to handle the bottleneck due to multiple deduplication pools should be factored and required documentation from the OEM is to be submitted along with the proposal.	No Change, Please be guided by the RFP
1238	10	Appendix-1B_TRS	Backup Solution	Backup & retrieval software, Backup Appliance or Integrated applaince is to be proposed at both DC & DR with all requisite licenses for both the sites separately.	Proposed Applinace should intedrate with at least 3 Backup ISVs like Commvault,Veeam, Zerto, Cohesity etc.	No Change, Please be guided by the RFP
1239	10	Appendix-1B_TRS	Backup Solution	Backup software should be able to replicate backed up data in de-duplicated format (for bandwidth optimization) to another site for compliance purposes, without the need of external replication tools. All necessary licenses for achieving consistent replication of backup data should be quoted.	Backup software and Backup Appliance/Backup Storage should be able to replicate backed up data in de-duplicated format (for bandwidth optimization) to another site for compliance purposes, without the need of external replication tools. All necessary licenses for achieving consistent replication of backup data should be quoted.	No Change, Please be guided by the RFP
1240	12	Appendix-1B_TRS	Long Term Storage	Proposed storage would be proposed for long retention of Backup data (Protocol-NAS/CIFS/SMB/S3/SAN storage (Protocol- iSCSI)	Purpose built backup applinace uses specialized backup protocol like OST-catalyst to provides higher data reduction effieciency and also provides Built-in Ransomeware protection features at Hardware Backup Repository level to protect the Backup copy. Purpose built backup applinace provides Data protection, Replication, Encryption, Immutability, MFA (Multi-factor authentication)/Dual Factor Authentication and Compliance mode etc. Hence request to change the clause to "Proposed storage would be purpose built backup Applinace and shall not be based on general purpse NAS or SAN Storage." OR change the clause to "Proposed storage would be proposed for long retention of Backup data (Protocol-NAS/CIFS/SMB/S3/SAN/Catalyst -Backup Appliance storage"	Please refer the addendum for revised clause
1241	158	13.3	At risk amount	The monthly At-Risk Amount (ARA') shall be 15% of the estimated monthly payout of the respective month	Bidder Request to clarify. If this amount is witheld as security, then request to delete this clasue as security deposits/ performace bank gurantee is already provided for the services as security.	No Change, Please be guided by the RFP
1242	163	14.15	Force Majeure	As per RFP	Bidder requests that the force majeure events are not only limited to [fires, floods, terrorism, war, etc.] but include any circumstances beyond a party's reasonable control.Invocation of Force Majeure provisions must not be linked to acceptance by either party of the said Force Majeure event.	No Change, Please be guided by the RFP
1243	165	14.19	Liquidated Damages	The Bank will consider the inability of the bidder to deliver or install the equipment & provide the services required within the specified time limit as a breach of contract and would entail the payment of Liquidated Damages on the part of the bidder. The liquidated damages represent an estimate of the loss or damage that the Bank may have suffered due to delay in performance of the obligations (relating to delivery, installation, operationalization, implementation, training, acceptance, warranty, maintenance etc. of the proposed solution/services) by the bidder. Installation will be treated as incomplete in one / all the following situations: Non-delivery of any component or other services mentioned in the order Non-delivery of supporting documentation Delivery / availability, but no installation of the components and/or software No integration/ Incomplete Integration Non-Completion of Transition within suggested timeline System operational, but not as per SLA, Timelines and scope of the RFP If the bidder fails to deliver any or all of the products and/or systems and/or services solutions within the time period(s) specified in the Delivery Schedule or installation, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as	Bidder request that any LD and penalties be recovered from the bidder at the end of the contract and not from the payments due to the bidder. Also, any failure or delay by Bidder will be excused if it was caused by: -Customer or Customer's affiliates, agents or contractors. -Force majeure event -Reliance on Customer instructions, authorisations, approvals or other information -A third party not under the control of HPE	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1244	New Clause Requested	New Clause Requested	Exclusion of implied warranties and exclusion of warranty claims.	Exclusion of implied warranties and exclusion of warranty claims.	HPE warrants that Deliverables will conform materially to their written specifications for 30 days following delivery. If Customer notifies HPE of a non-conformity during the 30 day period, HPE will promptly remedy the impacted deliverables or refund to Customer the fees paid for those deliverables and Customer will return those deliverables to HPE To the full extent permitted by law, HPE: (a) excludes all representations, warranties, terms and conditions, whether express or implied (and including those implied by statute, custom, law or otherwise), except as expressly set out in this Agreement; (b) does not give any warranty, representation or guarantee: (i) that any Deliverable, Product, advice, report, data or HPE Service is free from errors or will operate uninterrupted or error-free, (ii) that the HPE Services, Products or Deliverables will ensure or enable the achievement of any desired business results for Customer not documented in the agreed specifications All third party products are supplied in accordance with the third party's standard terms, including as to licences and warranties.	No Change, Please be guided by the RFP
1245	New Clause Requested	New Clause Requested	Transfer of Intellectual Property Rights for all customisations or new developments (IPR)	Absent	Each party retains ownership of its existing intellectual property, and no IP ownership is transferred under the contract. Both parties may use each other's IP only as needed to fulfill contractual obligations. Any deliverables created specifically for the purchaser may be used internally by the purchaser under a non-exclusive, royalty-free license after full payment.	No Change, Please be guided by the RFP
1246	98	Section 9 - Project Timelines	Overall implementation period	Overall Implementation period shall be 5 Months (Start Date is T0) for all solution & services.	Given the scope covers 14 solutions and 9 managed services with mandatory OEM-led implementation, hardware procurement lead times (60-90 days for servers/storage post-PO), and dependency on Bank environment readiness (network, firewall rules, log source onboarding), a 5-month window for all solutions is extremely challenging. Request the Bank to (a) extend the overall implementation period to 9-12 months, or (b) permit solution-wise phased Go-Live milestones (e.g., SIEM/SOAR/UEBA in Phase 1, remaining solutions in Phase 2) with LD applicability per phase rather than on the overall period. Please also confirm that delays attributable to the Bank, incumbent vendors, or third parties will extend timelines without LD.	No Change, Please be guided by the RFP.
1247	98	Section 8 - Contract Period	Contract period definition	The contract period is Implementation Period + Support period (60 Months Post Go-live).	Since solutions may go live on different dates, please confirm whether the 60-month support period commences (a) solution-wise from each solution's respective Go-Live date, or (b) from the final/last solution Go-Live date. This materially affects ATS/AMC/subscription sizing and pricing.	The 60 Month support period commences , solution wise from each solution's respective Go - Live dates
1248	95	Section 7.19.2 - Transition Management	Clause 2 & 3 - Operations take-over	The Bidder shall take over and maintain the operations and support of the Bank's existing solutions with effect from 01.05.2027 on an as-is and where-is basis... shall not exempt the Bidder from meeting the applicable SLAs.	Request the Bank to (a) share the complete inventory of existing solutions/OEMs, license validity, ATS/AMC status, EPS/sizing and known issues as a corrigendum, since bidders cannot price the take-over without this; (b) confirm who bears the license/ATS/OEM support costs of the existing solutions during the take-over period - the Bank or the bidder; (c) confirm that SLA penalties will not apply to failures attributable to legacy hardware/software defects, expired OEM support, or design limitations of the incumbent stack which the bidder did not supply; and (d) confirm a minimum 60-90 day SLA stabilization/grace period from take-over.	Details shall be shared with the successful bidder
1249	95	Section 7.19.2 - Transition Management	Clause 4 - Existing SIEM parallel run	The bidder shall run the existing SIEM on as-is/where-is basis for another 12 months from the date of Go-Live of the respective solutions.	Please confirm (a) whether the existing SIEM OEM license, ATS and infrastructure costs during this 12-month parallel run are borne by the Bank or must be factored by the bidder (if bidder, request the incumbent SIEM OEM name, version, EPS licensed and renewal cost be disclosed); (b) whether historical log data from the existing SIEM must be migrated into the new SIEM, and if so, the data volume and retention period to be migrated; and (c) which BOM line item this parallel-run effort should be quoted under.	Yes, the existing SIEM/SOC platform is operational and will be replaced under this RFP. No historical data migration from the existing SIEM is envisaged. The existing SIEM/SOC infrastructure and solution shall be operated and maintained by the bidder on an “as-is, where-is” basis during the parallel-run period, as required for compliance, at no additional cost to the Bank. The existing SIEM shall continue to be operated for a period of 12 months after Go-Live of the proposed SIEM, primarily to support regulatory, audit and transition requirements.
1250	137	Section 12 - Payment Terms	Payment milestones - build portion	Product License Cost: 50% on delivery, 20% on UAT, 30% on Go-Live. Product Implementation: 20/50/20/10.	For subscription/SaaS licenses, OEMs invoice 100% annually in advance upon subscription activation. Request the Bank to release 100% of the first-year subscription cost on delivery/activation of the subscription, or alternatively confirm milestone-linked payment applies only to perpetual licenses. Additionally, request Go-Live-linked payments (30%/20%) be released solution-wise on each solution's Go-Live rather than on overall project Go-Live.	No Change, Please be guided by the RFP
1251	139	Section 12.4 - ATS/Subscription & AMC Cost	Advance payment against 110% BG	Annually in Advance: Upon submission of a Bank Guarantee equivalent to 110% of the annual subscription/ATS cost... or Quarterly in Arrears.	The requirement of a 110% BG for annual-advance payment adds significant financing cost across a 5-year term with 14 solutions. Request the Bank to reduce the BG to 100% of the annual amount, or accept payment annually in advance against invoice without BG for OEM subscription renewals (which are non-refundable, non-cancellable OEM commitments).	No Change, Please be guided by the RFP
1252	146	Section 13.1 - SLA	Availability - 99.90% per component	Availability of each solution, Infrastructure Elements & Systems, any individual component - 99.90%. For every 0.05% or part thereof drop, penalty 1% of Monthly Maintenance Cost.	Measuring 99.90% at 'any individual component' level penalizes component-level events even where the solution remains fully available through the mandated N+N HA architecture. Request availability be measured at the solution/service level (end-user impact) rather than per individual component, with component failures covered under incident-resolution SLAs. Also request confirmation that downtime of one HA node with no service impact is excluded from availability calculation.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1253	143	Section 13.1 - Criticality Table	Critical incident resolution - 45 minutes	Critical/High: Response within 15 minutes, Resolution within 45 minutes (24x7x365). Classification includes failure of any production component.	A 45-minute resolution for all critical incidents is not achievable where resolution depends on OEM L4/engineering fixes, hardware part replacement, or root-cause-driven changes. Request (a) resolution SLA be redefined as 'restoration of service (including via workaround/failover)' with permanent fix timelines governed by OEM support case management; and (b) hardware replacement scenarios be aligned to the 4-hour repair/replace/standby clause (13.1.13) rather than 45 minutes.	No Change, Please be guided by the RFP
1254	148	Section 13.1 - Performance Measurements	Hardware/storage utilization thresholds	Daily peak utilization of CPU, memory, NIC, storage I/O exceeds 75% for more than 5 consecutive minutes... penalty 1% of MMC per incident. Storage utilization exceeding 80%.	Transient utilization peaks above 75% for 5 minutes are normal during backups, replication, correlation bursts, and scheduled scans, and do not indicate under-sizing. Request the threshold be revised to sustained utilization above 85% for 30+ consecutive minutes during business operations (excluding scheduled backup/maintenance windows), or measured as monthly average peak. Alternatively, confirm that scheduled activities (backup, replication, patching, VA scans) are excluded from utilization measurement.	No Change, Please be guided by the RFP
1255	150	Section 13.1 - DR Instance Availability	RPO 15 minutes / RTO 60 minutes	Restoration of business operations from the DR site within RTO 60 minutes and RPO 15 minutes.	Please confirm (a) the RTO/RPO applies to the NextGen SOC solutions supplied under this RFP only (not to Bank business applications); (b) inter-site bandwidth/latency between DC (Mumbai) and DR (Noida) will be provided by the Bank and is adequate for 15-minute RPO replication of ~2-3 TB/day log volumes - request the available bandwidth be specified; and (c) RTO measurement excludes time for Bank's decision/declaration of DR invocation.	No Change, Please be guided by the RFP
1256	156	Section 13.1 - Audit/VAPT Gaps	Highly Critical closure within 6 hours	Highly Critical: Within 6 hours from identification of the vulnerability; penalty INR 50,000 per 6 hours.	Vulnerability remediation frequently depends on OEM patch availability, and patches must undergo change management and non-production testing per the Bank's own policies (Section 7.13). Request (a) the 6-hour timeline apply to mitigation/compensating controls, with final patch closure per OEM patch-release timelines plus Bank change-approval; and (b) the clock start from Bank-approved change window rather than identification.	No Change, Please be guided by the RFP
1257	159	Section 14.1 - Assignment & Subcontracting	Subcontracting prohibition / payroll	The selected bidder shall not subcontract... All bidder's personnel proposed for the bank shall be on bidder's Payroll.	Large SIs deliver FM services through wholly-owned subsidiaries and group companies under common ownership and quality systems. Request the Bank to permit deployment of resources on the payroll of the bidder's wholly-owned subsidiaries/affiliates/group companies, with the bidder retaining single-point contractual responsibility. Please also confirm that OEM-certified partner engineers deputed by OEMs for implementation are covered under the OEM-personnel exclusion.	No Change, Please be guided by the RFP
1258	75	Section 7.12.4 - Minimum Resource Count	Minimum onsite deployment	Shift A: 4 L1, 2 L2, 1 L3/PM; Shift B: 4 L1, 2 L2; Shift C: 4 L1, 1 L2.	Please confirm (a) the minimum counts are per shift per day (i.e., 13 L1 + 5 L2 + 1 PM/L3 on any given day), and leave/weekly-off backup is over and above; (b) whether the L3/Project Manager for Shifts B and C may be provided on on-call basis; and (c) the resource deployment location(s) - Delhi (CISO Cell/STC), Mumbai DC, or Noida DR - and expected split, as this affects costing.	No Change, Please be guided by the RFP The Resource requirement given in the RFP is minimum mandatory requirement that is to be deployed. It includes both DC & DR. Bidder can propose the manpower over and above if required.
1259	72	Section 7.12.1/7.19.2 - Resources	Resource deployment start date	Bidder shall deploy required support resources at the Bank's premises with effect from 01.05.2027... onsite human resource from the date of NextGEN SOC solutions installation.	Please confirm whether the minimum O&M resource counts (7.12.4) apply in full from 01.05.2027 (take-over of existing solutions), or whether a reduced transition team is acceptable until Go-Live of the new solutions, with full deployment thereafter. Request the Bank specify the minimum team size expected during the take-over-only period, and which BOM line the take-over period manpower should be quoted under.	The existing SIEM/SOC platform is operational and will be replaced under this RFP. No data migration from the existing SIEM/SOC is envisaged. The existing platform shall run in parallel with the proposed solution for a limited period to meet compliance requirements. The Bidder shall not require to factor any existing OEM Services cost for such parallel operation period, support is to be provided on best effort basis. The Bidder shall ensure successful Go-Live of the proposed solution within the prescribed implementation timeline, irrespective of the parallel operation of the existing SIEM/SOC.
1260	89	Section 7.18 - IT Infrastructure	Clause 9/19 - Non-production environment	Bidder has to propose a dedicated non-production environment... production and non-production environment should be physically separate.	Clause 9 and 19 of Section 7.18 require physical separation of production and non-production compute, while Annexure 21 sizes non-production at minimum 10% of Production (DC) for VM-based solutions. Please confirm (a) non-production is required only for on-premises/appliance solutions (SaaS solutions being covered by OEM's native test tenants); (b) logical separation on dedicated hosts is acceptable; and (c) the 10% sizing basis applies to compute and storage.	Logical tenancy is acceptable, provided that the proposed bidder/OEM ensure clear separation and isolation of the Bank's data, security telemetry, logs, alerts, configurations, policies, analytics, investigation data and other Bank-related information from those of other tenants. The proposed environment for bank are protected against confidentiality and integrity risks and co-mingling of data and bidder/OEM implement adequate safeguards against combining of information, documents, records and assets.
1261	94	Section 7.19.1 - Other Scope	Clause 13 - Space and power	The hosting Space and Power arrangement shall be provided by the Bank at DC and DRC. However, the bidder is required to factor in the requisite racks.	Request the Bank to confirm (a) the number of racks, power (kW per rack) and cooling available at DC Mumbai and DR Noida for this project; (b) that structured cabling up to the rack, WAN/LAN connectivity, internet bandwidth for SaaS connectivity, and IP addressing are provided by the Bank; and (c) whether smart-hands support is available at DC/DR or bidder resources require permanent DC access.	No Change, Please be guided by the RFP
1262	258	Annexure 21 - Volumetrics	SIEM sizing - 50,000 EPS from outset	Total 50,000 sustainable EPS/2.06 TB per day (whichever is higher) of data ingestion from the outset scalable to 75,000 EPS/3.09 TB per day at DC & DR.	Please confirm (a) licensing is to be quoted for 50,000 EPS from day one, with 75,000 EPS as architectural scalability only (additional licenses procured via the 10,000 EPS tranche rates); (b) 'at DC & DR' means aggregate ingestion of 50,000 EPS across both sites and not 50,000 EPS at each site; and (c) the online/searchable (hot) retention period required in the SIEM platform - e.g., 90/180 days - since Annexure 21 specifies only backup retention. Online retention is the largest storage cost driver and must be uniform across bidders.	(a) Please refer addendum for the revised clause (b) 50,000 EPS / 2.81 TB per day represents the total required capacity. However, each DC/DR node/environment shall be independently provisioned to support the full peak load. (c) Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1263	40	Section 7.3.1.2 - SIEM EPS Measurement	EPS at ingestion boundary	EPS shall be measured at the SIEM ingestion boundary, after applicable source-side filtering... XDR native telemetry shall not be treated as additional SIEM EPS where not separately ingested.	We appreciate the clear EPS definition. Please additionally confirm that (a) events dropped/filtered at collectors per Bank-approved filtering policies are excluded from licensed EPS; and (b) if actual sustained ingestion exceeds the licensed 50,000 EPS due to growth in Bank log sources, the Bank will procure additional tranches at BOM rates and no SLA penalty applies for ingestion beyond licensed capacity until such procurement.	a) No Change, Please be guided by the RFP b) No Change, Please be guided by the RFP
1264	136	Section 11 - Right to Descope	Descope prior to award	The Bank reserves the right to... reduce, modify, defer, or descope one or more Solution Components... prior to issuance of the Contract/Letter of Award.	Since solutions share common underlay infrastructure (compute, storage, backup, virtualization) and integrated architecture, descoping one solution changes the cost basis of the remainder. Request confirmation that in the event of descope, the corresponding infrastructure, manpower and dependent line items will be equitably adjusted based on the bidder's impact notification, and the bidder will not be required to hold remaining prices where shared-cost allocation is materially affected.	Please refer the addendum for revised clause
1265	159	Section 14.2 - Right to Alter Quantities	+/-25% variation	The bank reserves the right... to increase or decrease the quantity... by up to twenty-five percent (25%)... without any change in the unit prices.	Request confirmation that (a) the 25% variation applies per line item at the quoted unit rates and within the contract period; and (b) for decreases, payment obligations for already-delivered/committed OEM subscriptions (which are non-cancellable) will be honoured.	No Change, Please be guided by the RFP
1266	157	Section 13.2 / 14.19 - LD	LD on implementation - 1% per week of Product Cost	Delay in delivery, installation... or any project milestone, LD of 1% per week of the respective Product Cost subject to maximum 10% of total contract value.	Request (a) LD be levied on the value of the delayed product/milestone only (as drafted) and capped at 10% of the respective product cost rather than referencing total contract value; (b) confirmation that LD and SLA penalties combined remain within the single overall 10% TCV cap (Section 13.2) and are not additive beyond it; and (c) LD excludes delays attributable to the Bank (site readiness, approvals, log-source access, UAT sign-off delays) and force majeure.	a) No Change, Please be guided by the RFP b) No Change, Please be guided by the RFP c) No Change, Please be guided by the RFP
1267	158	Section 13.3 - At-Risk Amount	ARA 15% of monthly payout	The monthly At-Risk Amount (ARA) shall be 15% of the estimated monthly payout of the respective month.	Please clarify the operation of the At-Risk Amount vis-a-vis SLA penalties: (a) does the ARA cap the maximum penalty deductible in any month at 15% of that month's payout; and (b) confirm ARA is not an additional deduction over and above computed SLA penalties.	The At-Risk Amount is a contractual performance mechanism and shall be withheld/adjusted in accordance with the applicable performance requirements specified in the RFP. It shall not automatically be treated as an additional penalty or Liquidated Damages (LD). Any withholding, adjustment or recovery under the At-Risk Amount shall be accounted for within the overall 10% penalty/LD cap specified in Section 13.2 and shall not be over and above such cap.
1268	146	Section 13.1 - MMC Definition	MMC formula divisor of 60	Monthly Maintenance Cost = (Total FM Cost + Total AMC Cost + Total ATS or Subscription Cost) / 60.	Since hardware carries a 3-year warranty (AMC only in Years 4-5) and subscription renewals for Years 4-5 are quoted separately, dividing the 5-year totals by 60 produces an MMC that does not reflect the actual monthly run-rate in early years. Request confirmation that MMC for penalty computation is based on the applicable charges of the respective year/quarter rather than a flat 60-month average, or clarify the intended computation.	No Change, Please be guided by the RFP
1269	27	Section 7.1 - Key Implementation Responsibilities	OEM-performed implementation	The implementation of each proposed solution... shall be performed by the respective OEM. The Bidder shall arrange OEM resources.	Global OEMs (particularly SaaS providers) deliver implementation through OEM Professional Services and/or OEM-certified delivery partners under OEM supervision. Request confirmation that implementation by OEM Professional Services or OEM-authorized/certified engineers (with the OEM issuing the deployment compliance certificate per the RFP) satisfies this requirement.	No Change, Please be guided by the RFP
1270	101	Section 10.2 - Eligibility Criteria	Clause 5 - MAF requirements	MAF should be submitted from the following solution OEMs: SIEM, SOAR, UEBA, XDR, NDR...	Where a single OEM platform natively provides multiple in-scope capabilities (e.g., SIEM+SOAR+UEBA on one platform, or XDR+ITDR from one OEM), please confirm (a) a single consolidated MAF from that OEM covering all such solutions is acceptable; and (b) proposing one OEM platform for multiple solution line items is permitted, with credentials counted for each respective solution in technical evaluation.	No Change, Please be guided by the RFP
1271	129	Section 10.3 - Technical Evaluation	Criteria 3 - OEM SIEM credentials	Category 3: 75000 EPS/3TB per day or more - Point 6: Client = 2 (of which 1 should be a Scheduled Commercial Bank) - 15 Marks.	For global SaaS SIEM OEMs, client-issued documents disclosing EPS of named Indian banks are often restricted by NDA. Request the Bank to accept (a) OEM-certified credential letters (on OEM letterhead, with client name and capacity) in lieu of client-issued POs, and/or (b) global (non-India) deployments for the capacity categories, with India presence demonstrated separately.	Please refer the Section10.2 Eligibility Evaluation Criteria. The documents requriement remains same for the technical evalaution as well.
1272	261	Annexure 21 - 16.21.3 Deployment & Data Retention	LTS retention for entire contract	Monthly Full backups shall be migrated to Long-Term Storage (LTS) at bank's DC & DR and retained for the entire duration of the contract.	To size LTS accurately, request confirmation of (a) the data sets in scope of monthly full backups (SIEM logs, solution configurations, databases) and the expected monthly full backup volume; (b) whether deduplication/compression-effective capacity sizing is acceptable; and (c) whether LTS at both DC and DR must each hold the full retention set (i.e., two complete copies).	Please refer addendum for the revised clause
1273	68	Section 7.7 - On-cloud OEM Responsibilities	Cloud data residency	All Bank data shall reside within India. No data shall be transmitted, processed, or stored outside India.	Certain SaaS security platforms process threat-intelligence enrichment/telemetry lookups via global cloud infrastructure while storing customer data in-country. Please confirm whether (a) India data residency applies to storage and processing of Bank log/event data (with anonymized/hashed threat-intel lookups permitted globally), or (b) strict in-country processing is mandated for all functions - in which case request the Bank confirm acceptance of solutions with India region SaaS hosting only.	No Change, Please be guided by the RFP
1274	21	Section 6.11 - PBG	PBG duration	5% of Project Cost... for the duration of the contract (Including the extension) + claim period (12 months).	A PBG covering the base term plus a potential 2-year extension plus 12-month claim period (up to ~8.5 years) attracts substantial BG charges even if no extension is exercised. Request the PBG validity be contract period + claim period, with extension coverage furnished as and when the Bank exercises the extension option.	The PBG shall be valid for the entire original Contract Period (i.e., Implementation Period + 60 months of Support Services), along with a claim period of 12 months. In case the Bank exercises its option to extend the Contract beyond the original Contract Period, for up to two (2) additional years in one-year increments, the Selected Bidder shall be required to extend the validity of the PBG corresponding to the extended Contract Period, along with the additional 12-month claim period.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1275	20	Section 6.10 - EMD	EMD exemption	Bidders who are eligible for EMD exemption as per GeM General Terms and Conditions are required to submit a Bid Security Declaration in lieu of EMD.	Please confirm the categories eligible for EMD exemption under this tender (MSE/Startup per GeM GTC) and that no other exemption categories apply. Also confirm whether EMD in the form of Bank Guarantee per Annexure 15 is acceptable in lieu of deposit.	No Change, Please be guided by the RFP for EMD Exemption . And Refer Addendum for the revised Annexure
1276	26	7.1	Scope and objective	"Any customization, enhancement, parser development, connector creation, workflow automation, dashboard customization, incident integration, playbook development, reporting customization, alert tuning, remediation activities, APIs, or native integrations required for successful implementation shall be provided without any additional cost to the Bank throughout the contract period."	The bidder is responsible for considering parser development, fine-tuning, customization, and related activities until implementation, as per the scope defined in the RFP. However, any customized parser requiring OEM Professional Services must go through a formal change request process. Kindly conduct price discovery for such Statements of Work (SoW).	No Change, Please be guided by the RFP
1277	26	7.1	(h) Compliance Requirements	"The proposed solution shall comply with the Bank's IT Policy, Information Security Policy, Cyber Security Policy, Cloud Security Policy, Data Governance Policy, Digital Payment Security Controls, and all other internal policies."	The scope of the RFP is fixed, and the bidder is expected to adhere strictly to the defined requirements. However, in the event of any specific requirement related to policy compliance that must be incorporated into the architecture, we request to provide appropriate suggestions.	No Change, Please be guided by the RFP
1278	256	16.21	Non-Production Environment	For VM-based solutions, the non-production environment shall be sized at a minimum of 10% of the Production (DC) environment... For appliance-based solutions, the bidder shall design and propose an appropriate non-production environment..."	Kindly specify whether you require non-production environments for each solution such as Decoy, Vulnerability Assessment (VA), Identity Lifecycle Management, CTEM, etc. These are passive monitoring solutions. If yes, please indicate the minimum requirements; otherwise, the respective OEMs will apply their own understanding when considering licenses. Our recommendation is to maintain non-production environments only for essential solutions.	Please refer addendum for revised clause
1279	35	7.2.4.1	Deployment Pattern	Item a,b,c,d: The core platforms shall be deployed in the Cloud/SaaS environment, with the required brokers, collectors, aggregators and/or integration/enforcement components deployed at the Bank's DC and DR in N+N Active- Active configuration. The Cloud/SaaS components shall be deployed with HA in accordance with the applicable SLA, RTO and RPO requirements.	Kindly clarify whether you require only a cloud-based solution, or if the bidder may also propose an on-premises solution.	Please refer addendum for the revised deployment architecture
1280	269	16..21.2 (6)	NDR	Throughput requirement of 10 Gbps All the inline components of the solution must operate in high availability mode. In the event of any component failure, the system should automatically initiate failover within seconds, ensuring uninterrupted functionality without requiring manual intervention. Each node/environment must be individually provisioned for full peak load	As we know NDR is a passive solution and doesn't work in HA hence kindly remove HA requirement from NDR.	No Change, Please be guided by the RFP
1281	57	7.4.6	Dark Web Monitoring	The Bidder shall provide offsite, tool-based continuous dark web and cyber threat exposure monitoring services to identify potential exposure of the Bank's sensitive information across the surface web, deep web, dark web, underground forums, messaging platforms, and data leak repositories.	For the darkweb monitoring can you help with the domains to be considered and no of takedowns to consider in the proposal	Detailed domain and identity information shall be provided to the selected bidder on a need-to-know basis
1282	64	7.6.6	Testing- Activities are to be performed by Respective solution OEM (supported by bidder)	The bidder shall provision and maintain dedicated Development, Testing, UAT, and Pre-Production environments throughout the contract period. All software, licenses, and other resources required for such environments shall be included within the bidder's scope without any additional cost to the Bank.	Can this be hosted in the OEM's cloud or is it required to be hosted in banks premises?	No Change, Please be guided by the RFP
1283	68	7.7		The proposed Cloud/SaaS solution shall support Bring Your Own Key (BYOK) and/or Customer-Managed Encryption Key (CMEK) capability, enabling the Bank to maintain control over the cryptographic keys used to protect its security data	Can this clause be relaxed or read as dedicated key for the customer to be provisioned with customer security policies enforced for the same?	No Change, Please be guided by the RFP
1284	73	7.12.3	2 OEM Implementation Resources	Onsite (Full Time) OEM shall submit a detailed resource deployment plan commencement of requirement gathering. Any replacement or modification shall require prior Bank approval.	Can this clause be relaxed or read as OEM resources to be available during the deployment phase only and be made available when needed?	No Change, Please be guided by the RFP
1285	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 23	XSIAM	Point 18	The proposed solution shall provide cloud-native high availability and redundancy mechanisms to tolerate failures of underlying infrastructure components without disruption to security monitoring and operational capabilities. The solution shall provide automated failover and service continuity within the cloud environment through the CSP's native availability and resiliency capabilities	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. "" The proposed solution shall provide cloud-native redundancy mechanisms to tolerate failures of underlying infrastructure components without disruption to security monitoring and operational capabilities. The solution shall provide automated failover and service continuity "	Please refer the addendum for revised clause
1286	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 23	XSIAM	Point 36	The proposed solution must come with out-of the-box/customized to be delivered on day 1 support integration and dashboards, reports, rules etc. to provides rapid insights and operational visibility into large-scale CentOS, Windows, Unix and Linux environments machine data.: syslog, metrics and configuration files.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The proposed solution must come with out-of the-box/customized to be delivered on day 1 support integration and dashboards, reports, rules etc. to provides rapid insights and operational visibility into large-scale CentOS, Windows, Linux environments machine data.: syslog, metrics and configuration files.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1287	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 24	XSIAM	Point 59	The proposed solution machine learning capabilities must allow addition or have inbuilt feature of custom machine learning algorithms from popular open-source libraries like NLP, Python etc.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The proposed solution must natively supports custom machine learning algorithms through its built-in Bring Your Own Machine Learning (BYOML) framework. This capability allows mature Security Operations Centers (SOCs) and security data scientists to access the massive security data lake stored within the platform and run bespoke analytics tailored to their specific environment.	No Change, Please be guided by the RFP
1288	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 37	XDR	Point 43	The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature or through seamless integration with a third-party sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature or through seamless integration with a third-party sandboxing solution from day 1.""	Please refer the addendum for revised clause
1289	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 1.4	Identity Threat Detection Solution must find and present high-risk attack pathways to critical IT assets	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. "ITDR provides identity risk context through User Risk View, Risk Management Dashboard, and identity alerts.	Please refer the addendum for revised clause
1290	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 1.6	Identity Threat Detection Solution should must automatically prioritize and remediate the riskiest identities to preemptively cut off what attackers need (and expect to find) to move undetected within the network.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. "ITDR identifies risky identities and supports remediation workflows for suspicious identity activity."	Please refer the addendum for revised clause
1291	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.3	The ITDR solution shall identify and assess exposed, improperly stored, or compromised credentials associated with user, privileged, service, and administrative identities on endpoints	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ITDR identifies risky identity posture, weak or compromised credentials, and suspicious activity involving user, privileged, service, and administrative accounts.	Please refer the addendum for revised clause
1292	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.4	Identity Threat Detection Solution should Identify, Misconfigured accounts, Legacy app accounts, Stale accounts, password policy violations, Kerberoastable credentials, unmanaged user accounts, unmanaged service accounts	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR identifies risky identity posture, weak or compromised credentials, Kerberoasting activity, and suspicious behavior involving service and administrative accounts""	Please refer the addendum for revised clause
1293	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.5	Identity Threat Detection Solution should Provide continuous monitoring and customizable, automated business rules to eliminate security policy violations, such as: • Stored credentials to sensitive assets • Local-admin accounts • Cached credentials stored in browsers, Windows and other systems	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR continuously monitors identity posture and access relationships to identify risky configurations, excessive privileges, and suspicious identity activity across Active Directory and related identity sources.""	Please refer the addendum for revised clause
1294	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.7	Identity Threat Detection Solution should be available through rack-mountable on-premise deployment	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Identity Threat Detection Solution should be available through rack-mountable on-premise deployment not applicable for SaaS solution ""	Please refer the addendum for revised clause
1295	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.9	Identity Threat Detection Solution should detect all types of attack vectors including but not limited to pre attack reconnaissance,zero- day attacks, privilege escalation prevention, lateral movement, data theft	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR detects identity-based threats such as Active Directory reconnaissance, compromised accounts, privilege escalation, and anomalous access, while providing identity context to help investigate exposure and attack paths.""	The Clause is applicable only to idendity related threat vector only. The volumetrics is provided in the RFP and should be complied
1296	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.15	Identity Threat Detection controls should be able to automatically discover and flag hidden or shadow Tier 0 assets	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Identity Threat Detection and Response helps identify risky identity assets, excessive privileges, and exposure across identity relationships.""	Please refer the addendum for revised clause
1297	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.17	Identity Threat Detection Solution should be able to pull and analyze identity data from AD, Entra ID, identity stores, PAM systems	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR analyzes identity data from supported identity sources, including Active Directory and Microsoft Entra ID, to provide context on identities, permissions, and access exposure""	Please refer the addendum for revised clause
1298	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 3.4	The Identity Threat Detection Solution should integrate with compatible endpoint/extended detection solution to capture screen recordings or screenshots during active attacker sessions, as part of advanced forensic evidence collection	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR integrates with supported tools to share identity and endpoint context for investigation and response, including forensic collection where available.""	Please refer the addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1299	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 3.5	The Identity Threat Detection Solution should integrate with compatible network detection solution to support collection of PCAP data to support network-level visibility of the incident	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR integrates with supported tools to share identity risk context and support investigation workflows, including network-related telemetry where available.""	Please refer the addendum for revised clause
1300	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 53	ITDR	Point 3.7	Identity Threat Detection Solution should, as part of its forensic data collection process, include detailed attack path information, including the protocols leveraged during the attack.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR provides identity context through asset, permission, and authentication analysis, and detects identity-based threats such as compromised accounts, privilege escalation, anomalous access, and Active Directory reconnaissance.""	Please refer the addendum for revised clause
1301	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 53	ITDR	Point 3.9	Identity Threat Detection solution should detect an adversary's attempt to move laterally toward the organization's key assets using as many hosts (Windows, Mac, or Linux) as possible in the organization without requiring a persistent agent.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Identity Threat Detection solution should detect an adversary's attempt to move laterally toward the organization's key assets using as many hosts (Windows, Mac, or Linux) as possible in the organization With or without requiring a persistent agent.""	Please refer the addendum for revised clause
1302	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 53	ITDR	Point 3.10	Identity Threat Detection Solution should collect user and computer information from Active Directory as part of its forensic data gathering to enhance context and assess risk exposure. detect at the earliest point in the attack, post initial compromise as the attacker is first attempting to move laterally and escalate privilege.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR collects and analyzes identity data to improve context and assess risk exposure. It detects identity-based threats, including compromised accounts, privilege escalation, anomalous access, and Active Directory reconnaissance, early in the attack path.""	Please refer the addendum for revised clause
1303	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 53	ITDR	Point 3.11	Identity Threat Detection Solution should collect user and computer data from Active Directory during forensic data gathering to improve context and evaluate risk exposure, while ensuring that all deception techniques remain hidden from legitimate users.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Identity Threat Detection and Response collects and analyzes identity data to improve context and assess risk exposure. It provides deep visibility into identity assets, permissions, relationships, and authentication activity across Active Directory and other identity sources. ITDR also supports forensic investigations through endpoint data collection and analysis."	Please refer the addendum for revised clause
1304	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 19	CTEM	Point 7	Each intelligence item should include metadata such as date, author, source, and pre-classification of raw data	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Intelligence items include enriched context, source information, and analysis metadata to support investigation and prioritization.""	Please refer the addendum for revised clause
1305	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 19	CTEM	Point 11	The solution/service should generate investigation reports for designated VIPs or other high-risk identities/assets, providing an overview of identified digital exposure and associated risk.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution provides risk context and investigation views for identities and assets, helping analysts assess exposure and related risks.""	No Change, Please be guided by the RFP
1306	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 19	CTEM	Point 19	The solution should detect compromised credentials for employees and VIPs, exposed payment card information, and aggregate data from known breach databases in real time	Kindly Remove this clause for larger participation	Please refer addendum for revised clause
1307	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 20	CTEM	Point 38	The solution should be deployed agentlessly, without requiring sensors or agents on endpoints, servers, or network appliances	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution should be deployed agentlessly, With or without requiring sensors or agents on endpoints, servers, or network appliances""	Please refer the addendum for revised clause
1308	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 81	ASM	Point 6	The visual representations should be downloadable in PDF, JPG, PNG and other generally used formats	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution supports exporting reports and data views in supported file formats such as PDF, CSV, TSV, JSON, or ZIP, depending on the workflow""	No Change, Please be guided by the RFP
1309	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 81	ASM	Point 8	The solution shall provide information on vulnerabilities, misconfigurations, insecure configurations, obsolete or unsupported technologies, applications, services, URLs, ports, network components, systems, databases and other relevant infrastructure that are publicly exposed or otherwise identifiable through authorized discovery and assessment activities.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution provides exposure information for internet-facing assets, including vulnerabilities, misconfigurations, services, and related attribution data discovered through authorized asset mapping and assessment.""	Please refer addendum for revised clause
1310	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 81	ASM	Point 9	The solution should provide data/information on security flaws/ inherent vulnerabilities (allegedly) reported about the digital products exposed to the Internet (For example: internet banking, mobile applications) offered to the bank's customers, as leaked in public domain, or other forums	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution provides exposure and risk information for internet-facing digital assets, including vulnerabilities, services.""	No Change, Please be guided by the RFP The requirement is intended to provide visibility not only into directly identified technical vulnerabilities but also into relevant security information concerning the Bank's internet-facing digital products

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1311	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 81	ASM	Point 10	The solution shall identify and provide relevant information on potentially exposed sensitive information associated with the Bank, including source-code references, code snippets, API information, credentials, keys and other security-relevant information, where such information is identifiable through publicly available sources, external attack-surface intelligence or other authorized discovery mechanisms.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution provides exposure information for internet-facing assets, including vulnerabilities, misconfigurations, code weaknesses, and exposed secrets discovered through attack surface.""	Please refer addendum for revised clause
1312	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 54	Cloud security	Point 4	The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud environment like AWS/Azure/GCP/Meghdoot, AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud environment like AWS/Azure/GCP/, AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.	The requirement is intended for identification and contextualization of potentially exposed sensitive information associated with the Bank
1313	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 55	Cloud security	Point 9 (Sub point)	○Automatic, in-product remediation via the Cloud Service Provider (CSP) API (1-click)	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution supports in-product remediation workflows, including automated actions and approval-based playbooks where configured.	Please refer the addendum for revised clause
1314	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 56	Cloud security	Point 25	The solution must provide an self-service portal for engineers. The admin portal should be able to define the eligibility for users and groups, based on role, scope and duration. The solution should provide approval workflow and audit logs	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation." The solution supports granular access control, human approval in select workflows, and audit logging for access-related changes.	Please refer the addendum for revised clause
1315	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 40	NDR	Point 9	Easy-to-manage, clientless platform that deploys quickly and involves minimal or no dependency on customization and management.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Easy-to-manage, clientbase clientless platform that deploys quickly and involves minimal or no dependency on customization and management.""	Please refer the addendum for revised clause
1316	RFP Pg 35	Deployment Pattern	Point d	NDR: The NDR solution shall be deployed On-Premises within the Bank's DC and DR, with the required brokers, aggregators, collectors and/or enforcement components configured in N+N Active-Active configuration at both sites.	The proposed NDR solution shall utilize a hybrid deployment model or SaaS model.With the required brokers/ aggregators/collectors /Sensors and enforcement components configured in N+N Active-Active or Active- Passive configuration at both sites DC and DR.	Please refer addendum for the revised clause
1317	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 40	NDR			Clarification: Kindly confirm the specific physical interface type and speed the Bank will provide for the uplink to the NDR sensor.	Details shall be shared with successful bidder
1318	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 40	NDR	Point 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	"We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. "" The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead.""	Please refer Addendum for revised clause
1319	SELECTION OF BIDDER FOR SUPPLY INSTALLATION, IMPLEMENTATION, MAINTENANCE & MANAGEMENT OF NEXTGEN SOC & RELATED SERVICES BID NO: PSB/ HO-CISO CELL/2026-27/RFP_01 DATED 09/09/2026 Page 68	7.7 On-cloud proposed solution OEM Responsibilities	Page 8	The solution shall support secure connectivity with the Bank's on-premises infrastructure,cloud environments, and external systems through private and secure communication mechanisms.	SIEM is a SaaS solution accessible over the internet using passwords and multi-factor authentication and Https. However, access to your Cortex XSIAM tenant can be restricted based on your Bank's static public IP addresses. Kinkdy change this clause to "" The solution shall support secure connectivity with the Bank's on-premises infrastructure,cloud environments, and external systems through private or secure communication mechanisms via internet or tenant can be restricted based on Bank's static public IP addresses..""	Please refer the addendum for revised clause
1320	RFP Pg 33	Section 7.2.3 Deployment Model Definition		CSP-hosted components shall provide cloud-native High Availability (HA), geographic resiliency and DR in accordance with the SLA, RTO and RPO requirements specified in this RFP.	Cortex XSIAM is pure SaaS Solution hence this clause is not applicable. kindly remove this for SaaS offerings.	Please refer addendum for the revised deployment architecture
1321	RFP Pg 41	7.3.1.1 Modules, Architecture & Deployment:	Point 7	All SIEM components, including collectors, ingestion nodes, correlation engines, processing nodes, etc., are deployed in the prescribed HA architecture irrespective of whether they are deployed at the Bank's Data Centre (DC), Disaster Recovery (DR) Centre, CSP Primary Site, or CSP Secondary Site.	Not applicable, as Cortex XSIAM is a SaaS solution. However, the on-premises Cortex Broker VM component can be deployed in a High Availability (HA) configuration across primary Data Center (DC) and Disaster Recovery (DR) sites	For SaaS-based components, the applicable SaaS SLA shall specify the required uptime/availability commitment. For components deployed at the Bank's DC/DR, the prescribed HA architecture shall apply as specified in the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1322	RFP Pg 43	7.3.2.2 Key Deliverables	Point 7	Backup, retention, restoration, documentation and knowledge transfer for configured security automation capabilities and use cases.	Bidder request for more clarity on this clause	No Change, Please be guided by the RFP Refer Section7.2.4.3 Storage and other Requirement
1323	30	7.2.1	Identity Threat Detection & Response (ITDR)	On- Premises	Bidder request to Kindly Allow SaaS based solution also because no proven OEM solution available on-prem.	Please be refer addendum for revised clause
1324	137	12. Product License Cost	Payment Terms	On successful delivery of the licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware. The Bidder is required to submit the required to submit the following: Delivery proof OOTB Installation Proof Invoice of the Product	We request the Bank to kindly release 90% of the Product License Cost upon successful delivery of the licenses, once the software with OOTB features is made available for view and review by the Bank on the proposed hardware. Justification: The Product Licenses are procured from the OEM, which requires substantial upfront payment for license provisioning and activation. Accordingly, the Bidder has to make significant upfront financial commitments prior to delivery. Releasing 90% of the license cost upon successful delivery will align the payment milestone with the OEM's commercial terms and facilitate timely license provisioning and project execution.	No Change, Please be guided by the RFP
1325				On successful UAT Signoff of the respective product	We request the Bank to kindly release the remaining 10% of the Product License Cost upon successful UAT Sign-off of the respective product. Justification: This milestone aligns the balance payment with the successful completion and acceptance of UAT, ensuring that the final payment is released only upon successful validation and sign-off of the respective product by the Bank.	No Change, Please be guided by the RFP
1326	137	12. Product Implementation Cost	Payment Terms	On Successful installation of OOTB product on the sourced hardware and handing over the environment with OOTB product to Bank	We request the Bank to kindly revise the payment milestone from 20% to 50% upon successful installation of the OOTB product on the sourced hardware and handing over of the environment with the OOTB product to the Bank. Justification: This milestone represents the completion of a significant portion of the implementation activities and involves substantial upfront deployment of manpower, technical resources and implementation efforts. Revising the milestone to 50% will better align the payment with the actual effort and resources deployed at this stage.	No Change, Please be guided by the RFP
1327			Payment Terms	On successful UAT Signoff of the respective product	We request the Bank to kindly release 30% of the Product Implementation Cost upon successful UAT Sign-off of the respective product. Justification: UAT Sign-off confirms the successful completion and acceptance of the implemented product. Linking 30% payment to this milestone ensures that the payment is aligned with a key project acceptance milestone and successful validation by the Bank.	No Change, Please be guided by the RFP
1328			Payment Terms	On successful Go-live of the respective product	We request the Bank to kindly release 10% of the Product Implementation Cost upon successful Go-Live of the respective product. Justification: Go-Live marks the successful deployment and commencement of production operations. Linking 10% payment to this milestone ensures that the payment is aligned with the successful completion of implementation and transition to production.	No Change, Please be guided by the RFP
1329	137	12. Subscription Cost (One time license Cost)	Payment Terms	On successful delivery of the Licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware. The Bidder is required to submit the required to submit the following: Delivery proof OOTB Installation Proof Invoice of the Product	We request the Bank to kindly revise the payment milestone from 50% to 80% upon successful delivery of the Licenses, once the software with OOTB features is made available for view and review by the Bank on the proposed hardware. Justification: The licenses involve significant upfront financial commitment towards OEM provisioning and activation. Revising the milestone to 80% upon successful delivery will help align the payment with the upfront OEM payment obligations and license delivery, while the remaining 20% remains linked to successful UAT Sign-off.	No Change, Please be guided by the RFP
1330				On successful UAT Signoff of the respective product	We request the Bank to kindly release the remaining 20% of the Subscription Cost (One-time License Cost) upon successful UAT Sign-off of the respective product. Justification: Linking the balance 20% payment to successful UAT Sign-off ensures that the final payment is tied to the successful validation and acceptance of the respective product by the Bank, providing an appropriate acceptance-based milestone.	No Change, Please be guided by the RFP
1331	137	12. Appliance Cost	Payment Terms	On successful Delivery of the Appliance which would be considered delivered once the solution (with OOTB features) is made available for view and review of the bank. The Bidder is required to submit the required to submit the following: Delivery proof OOTB Installation Proof Invoice of the Product	We request the Bank to kindly revise the payment milestone from 50% to 80% upon successful delivery of the Appliance, once the solution with OOTB features is made available for view and review by the Bank. Justification: The Appliance involves substantial upfront procurement and OEM-related costs. Revising the milestone to 80% upon successful delivery will help align the payment with the significant financial commitment incurred for procurement and delivery, while the balance payment remains linked to subsequent project milestones.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1332				On successful UAT Signoff of the respective product	We request the Bank to kindly release 10% of the Appliance Cost upon successful UAT Sign-off of the respective product. Justification: UAT Sign-off confirms the successful validation and acceptance of the solution by the Bank. Linking 10% payment to this milestone ensures that the payment is aligned with a clear and objective project acceptance milestone.	No Change, Please be guided by the RFP
1333				On successful Go-live of the respective product	We request the Bank to kindly release 10% of the Appliance Cost upon successful Go-Live of the respective product. Justification: Go-Live marks the successful deployment and commencement of production operations. Linking 10% payment to this milestone ensures that the payment is aligned with the successful completion of implementation and transition to production.	No Change, Please be guided by the RFP
1334	137	12. Hardware Cost (Other than Appliances)	Payment Terms	Delivery (power on) of hardware and submission of invoice with Proof of Delivery and other documents of the hardware supplied. Bank may at its discretion verify the details before releasing the payment (This verification, if required, shall be completed within 1 month of delivery of the hardware on the bank's premises).	We request the Bank to consider 80% payment upon delivery (power-on) of the hardware, against submission of the invoice, Proof of Delivery (POD), and other required documents, as specified in the RFP. Justification: The proposed hardware involves substantial upfront procurement and OEM-related costs, which are generally payable by the bidder at the time of procurement or delivery. Releasing 80% payment upon successful delivery and submission of the required documents will help us manage the procurement cash flow and meet the project delivery commitments effectively. The requested payment milestone is directly linked to the successful delivery of the hardware and submission of the necessary supporting documents, thereby ensuring transparency and accountability in the payment process.	No Change, Please be guided by the RFP
1335				On successful installation of proposed solutions on the hardware - 50% of the sought product/solutions	We request the Bank to consider 10% payment upon successful installation and acceptance of 50% of the proposed solutions on the hardware, subject to the completion of the agreed installation milestone. Justification: The installation of the proposed solutions involves coordination among the OEM, implementation team, and the Bank. Linking the payment to the successful installation and acceptance of 50% of the proposed solutions will ensure that the payment milestone is aligned with measurable project progress and the successful delivery of the corresponding solution components. This arrangement will support effective project execution, resource planning, and timely delivery while maintaining a clear milestone-based payment structure.	No Change, Please be guided by the RFP
1336				On successful installation of remaining proposed solution on the hardware – remaining 50% of the sought product/solutions	We request the Bank to consider 10% payment upon successful installation and commissioning of the remaining 50% of the proposed solutions on the hardware. Justification: The remaining solution components involve additional OEM coordination, implementation efforts, technical resources, and associated project execution costs. Linking the payment to the successful installation and commissioning of the remaining solution components will align the payment with the actual completion of the corresponding project milestone and support timely resource deployment and project execution.	No Change, Please be guided by the RFP
1337	137	12. FM Manpower Cost	Payment Terms	Submission of SLA report and Submission of attendance record/register of Onsite resources on Quarterly basis	We request the Bank to consider monthly payment in advance for FM manpower services, against deployment of the agreed manpower/resources. Justification: FM manpower involves recurring monthly costs towards salaries, statutory benefits, and resource deployment. These costs are incurred by the bidder on a monthly basis irrespective of the quarterly billing cycle. Therefore, monthly advance payment will help ensure timely salary and statutory payments, maintain continuous manpower deployment, and ensure uninterrupted FM services throughout the contract period. The requested payment term will also align the payment cycle with the actual monthly cost incurred for manpower resources.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1338	165	14.21	Liquidated Damages	The Bank will consider the inability of the bidder to deliver or install the equipment & provide the services required within the specified time limit as a breach of contract and would entail the payment of Liquidated Damages on the part of the bidder. The liquidated damages represent an estimate of the loss or damage that the Bank may have suffered due to delay in performance of the obligations (relating to delivery, installation, operationalization, implementation, training, acceptance, warranty, maintenance etc. of the proposed solution/services) by the bidder. Installation will be treated as incomplete in one / all the following situations: 1. Non-delivery of any component or other services mentioned in the order 2. Non-delivery of supporting documentation 3. Delivery / availability, but no installation of the components and software 4. No integration/ Incomplete Integration 5. Non-Completion of Transition within suggested timeline 6. System operational, but not as per SLA, Timelines and scope of the RFP If the bidder fails to deliver any or all of the products, systems and services solutions within the time period(s) specified in the Delivery Schedule or installation, the Bank shall, without	We request the Bank to kindly consider revising the maximum Liquidated Damages cap from 10% to 5% of the total contract value. Justification: The proposed solution involves multiple activities, including hardware delivery, installation, integration, implementation, and other dependencies that may require coordination with the Bank, OEMs, and other stakeholders. Delays in certain activities may also arise due to factors beyond the bidder's reasonable control. A maximum LD cap of 5% of the total contract value would provide a more proportionate and reasonable allocation of risk while continuing to protect the Bank against genuine delays attributable to the bidder. The proposed cap will also maintain an appropriate balance between contractual accountability and the commercial risks associated with project execution.	No Change, Please be guided by the RFP
1339	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 23	XSIAM	Point 18	The proposed solution shall provide cloud-native high availability and redundancy mechanisms to tolerate failures of underlying infrastructure components without disruption to security monitoring and operational capabilities. The solution shall provide automated failover and service continuity within the cloud environment through the CSP's native availability and resiliency capabilities	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. "" The proposed solution shall provide cloud-native redundancy mechanisms to tolerate failures of underlying infrastructure components without disruption to security monitoring and operational capabilities. The solution shall provide automated failover and service continuity "	Please refer the addendum for revised clause
1340	9	XSIAM	Point 36	The proposed solution must come with out-of the-box/customized to be delivered on day 1 support integration and dashboards, reports, rules etc. to provides rapid insights and operational visibility into large-scale CentOS, Windows, Unix and Linux environments machine data.: syslog, metrics and configuration files.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The proposed solution must come with out-of the-box/customized to be delivered on day 1 support integration and dashboards, reports, rules etc. to provides rapid insights and operational visibility into large-scale CentOS, Windows, Linux environments machine data.: syslog, metrics and configuration files.	No Change, Please be guided by the RFP
1341	10	XSIAM	Point 59	The proposed solution machine learning capabilities must allow addition or have inbuilt feature of custom machine learning algorithms from popular open-source libraries like NLP, Python etc.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The proposed solution must natively supports custom machine learning algorithms through its built-in Bring Your Own Machine Learning (BYOML) framework. This capability allows mature Security Operations Centers (SOCs) and security data scientists to access the massive security data lake stored within the platform and run bespoke analytics tailored to their specific environment.	No Change, Please be guided by the RFP
1342	11	XDR	Point 43	The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature or through seamless integration with a third-party sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature or through seamless integration with a third-party sandboxing solution from day 1.""	Please refer the addendum for revised clause
1343	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 1.4	Identity Threat Detection Solution must find and present high-risk attack pathways to critical IT assets	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. "ITDR provides identity risk context through User Risk View, Risk Management Dashboard, and identity alerts.	Please refer the addendum for revised clause
1344	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 1.6	Identity Threat Detection Solution should must automatically prioritize and remediate the riskiest identities to preemptively cut off what attackers need (and expect to find) to move undetected within the network.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. "ITDR identifies risky identities and supports remediation workflows for suspicious identity activity."	Please refer the addendum for revised clause
1345	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.3	The ITDR solution shall identify and assess exposed, improperly stored, or compromised credentials associated with user, privileged, service, and administrative identities on endpoints	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ITDR identifies risky identity posture, weak or compromised credentials, and suspicious activity involving user, privileged, service, and administrative accounts.	Please refer the addendum for revised clause
1346	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.4	Identity Threat Detection Solution should Identify, Misconfigured accounts, Legacy app accounts, Stale accounts, password policy violations, Kerberoastable credentials, unmanaged user accounts, unmanaged service accounts	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR identifies risky identity posture, weak or compromised credentials, Kerberoasting activity, and suspicious behavior involving service and administrative accounts""	Please refer the addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1347	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.5	Identity Threat Detection Solution should Provide continuous monitoring and customizable, automated business rules to eliminate security policy violations, such as: • Stored credentials to sensitive assets • Local-admin accounts • Cached credentials stored in browsers, Windows and other systems	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR continuously monitors identity posture and access relationships to identify risky configurations, excessive privileges, and suspicious identity activity across Active Directory and related identity sources.""	Please refer the addendum for revised clause
1348	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.7	Identity Threat Detection Solution should be available through rack-mountable on-premise deployment	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Identity Threat Detection Solution should be available through rack-mountable on-premise deployment not applicable for SaaS solution ""	Please refer the addendum for revised clause
1349	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.9	Identity Threat Detection Solution should detect all types of attack vectors including but not limited to pre attack reconnaissance,zero- day attacks, privilege escalation prevention, lateral movement, data theft	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR detects identity-based threats such as Active Directory reconnaissance, compromised accounts, privilege escalation, and anomalous access, while providing identity context to help investigate exposure and attack paths.""	The Clause is applicable only to idendity related threat vector only. The volumetrics is provided in the RFP and should be complied
1350	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.15	Identity Threat Detection controls should be able to automatically discover and flag hidden or shadow Tier 0 assets	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Identity Threat Detection and Response helps identify risky identity assets, excessive privileges, and exposure across identity relationships.""	Please refer the addendum for revised clause
1351	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.17	Identity Threat Detection Solution should be able to pull and analyze identity data from AD, Entra ID, identity stores, PAM systems	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR analyzes identity data from supported identity sources, including Active Directory and Microsoft Entra ID, to provide context on identities, permissions, and access exposure""	Please refer the addendum for revised clause
1352	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 3.4	The Identity Threat Detection Solution should integrate with compatible endpoint/extended detection solution to capture screen recordings or screenshots during active attacker sessions, as part of advanced forensic evidence collection	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR integrates with supported tools to share identity and endpoint context for investigation and response, including forensic collection where available.""	Please refer the addendum for revised clause
1353	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 3.5	The Identity Threat Detection Solution should integrate with compatible network detection solution to support collection of PCAP data to support network-level visibility of the incident	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR integrates with supported tools to share identity risk context and support investigation workflows, including network-related telemetry where available.""	Please refer the addendum for revised clause
1354	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 53	ITDR	Point 3.7	Identity Threat Detection Solution should, as part of its forensic data collection process, include detailed attack path information, including the protocols leveraged during the attack.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR provides identity context through asset, permission, and authentication analysis, and detects identity-based threats such as compromised accounts, privilege escalation, anomalous access, and Active Directory reconnaissance.""	Please refer the addendum for revised clause
1355	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 53	ITDR	Point 3.9	Identity Threat Detection solution should detect an adversary's attempt to move laterally toward the organization's key assets using as many hosts (Windows, Mac, or Linux) as possible in the organization without requiring a persistent agent.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Identity Threat Detection solution should detect an adversary's attempt to move laterally toward the organization's key assets using as many hosts (Windows, Mac, or Linux) as possible in the organization With or without requiring a persistent agent.""	Please refer the addendum for revised clause
1356	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 53	ITDR	Point 3.10	Identity Threat Detection Solution should collect user and computer information from Active Directory as part of its forensic data gathering to enhance context and assess risk exposure. detect at the earliest point in the attack, post initial compromise as the attacker is first attempting to move laterally and escalate privilege.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR collects and analyzes identity data to improve context and assess risk exposure. It detects identity-based threats, including compromised accounts, privilege escalation, anomalous access, and Active Directory reconnaissance, early in the attack path.""	Please refer the addendum for revised clause
1357	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 53	ITDR	Point 3.11	Identity Threat Detection Solution should collect user and computer data from Active Directory during forensic data gathering to improve context and evaluate risk exposure, while ensuring that all deception techniques remain hidden from legitimate users.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Identity Threat Detection and Response collects and analyzes identity data to improve context and assess risk exposure. It provides deep visibility into identity assets, permissions, relationships, and authentication activity across Active Directory and other identity sources. ITDR also supports forensic investigations through endpoint data collection and analysis."	Please refer the addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1358	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 19	CTEM	Point 7	Each intelligence item should include metadata such as date, author, source, and pre-classification of raw data	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Intelligence items include enriched context, source information, and analysis metadata to support investigation and prioritization.""	Please refer the addendum for revised clause
1359	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 19	CTEM	Point 11	The solution/service should generate investigation reports for designated VIPs or other high-risk identities/assets, providing an overview of identified digital exposure and associated risk.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution provides risk context and investigation views for identities and assets, helping analysts assess exposure and related risks.""	No Change, Please be guided by the RFP
1360	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 19	CTEM	Point 19	The solution should detect compromised credentials for employees and VIPs, exposed payment card information, and aggregate data from known breach databases in real time	Kindly Remove this clause for larger participation	Please refer addendum for revised clause
1361	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 20	CTEM	Point 38	The solution should be deployed agentlessly, without requiring sensors or agents on endpoints, servers, or network appliances	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution should be deployed agentlessly, With or without requiring sensors or agents on endpoints, servers, or network appliances""	Please refer the addendum for revised clause
1362	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 81	ASM	Point 6	The visual representations should be downloadable in PDF, JPG, PNG and other generally used formats	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution supports exporting reports and data views in supported file formats such as PDF, CSV, TSV, JSON, or ZIP, depending on the workflow""	No Change, Please be guided by the RFP
1363	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 81	ASM	Point 8	The solution shall provide information on vulnerabilities, misconfigurations, insecure configurations, obsolete or unsupported technologies, applications, services, URLs, ports, network components, systems, databases and other relevant infrastructure that are publicly exposed or otherwise identifiable through authorized discovery and assessment activities.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution provides exposure information for internet-facing assets, including vulnerabilities, misconfigurations, services, and related attribution data discovered through authorized asset mapping and assessment.""	Please refer addendum for revised clause
1364	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 81	ASM	Point 9	The solution should provide data/information on security flaws/ inherent vulnerabilities (allegedly) reported about the digital products exposed to the Internet (For example: internet banking, mobile applications) offered to the bank's customers, as leaked in public domain, or other forums	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution provides exposure and risk information for internet-facing digital assets, including vulnerabilities, services.""	No Change, Please be guided by the RFP The requirement is intended to provide visibility not only into directly identified technical vulnerabilities but also into relevant security information concerning the Bank's internet-facing digital products
1365	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 81	ASM	Point 10	The solution shall identify and provide relevant information on potentially exposed sensitive information associated with the Bank, including source-code references, code snippets, API information, credentials, keys and other security-relevant information, where such information is identifiable through publicly available sources, external attack-surface intelligence or other authorized discovery mechanisms.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution provides exposure information for internet-facing assets, including vulnerabilities, misconfigurations, code weaknesses, and exposed secrets discovered through attack surface.""	Please refer addendum for revised clause
1366	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 54	Cloud security	Point 4	The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud environment like AWS/Azure/GCP/Meghdoot, AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud environment like AWS/Azure/GCP/, AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.	The requirement is intended for identification and contextualization of potentially exposed sensitive information associated with the Bank
1367	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 55	Cloud security	Point 9 (Sub point)	○Automatic, in-product remediation via the Cloud Service Provider (CSP) API (1-click)	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution supports in-product remediation workflows, including automated actions and approval-based playbooks where configured.	Please refer the addendum for revised clause
1368	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 56	Cloud security	Point 25	The solution must provide an self-service portal for engineers. The admin portal should be able to define the eligibility for users and groups, based on role, scope and duration. The solution should provide approval workflow and audit logs	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation." The solution supports granular access control, human approval in select workflows, and audit logging for access-related changes.	Please refer the addendum for revised clause
1369	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 40	NDR	Point 9	Easy-to-manage, clientless platform that deploys quickly and involves minimal or no dependency on customization and management.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Easy-to-manage, clientbase clientless platform that deploys quickly and involves minimal or no dependency on customization and management.""	Please refer the addendum for revised clause
1370	RFP Pg 35	Deployment Pattern	Point d	NDR: The NDR solution shall be deployed On-Premises within the Bank's DC and DR, with the required brokers, aggregators, collectors and/or enforcement components configured in N+N Active-Active configuration at both sites.	The proposed NDR solution shall utilize a hybrid deployment model or SaaS model.With the required brokers/ aggregators/collectors /Sensors and enforcement components configured in N+N Active-Active or Active- Passive configuration at both sites DC and DR.	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1371	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 40	NDR			Clarification: Kindly confirm the specific physical interface type and speed the Bank will provide for the uplink to the NDR sensor.	Details shall be shared with successful bidder
1372	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 40	NDR	Point 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	"We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. "" The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead.""	Please refer Addendum for revised clause
1373	SELECTION OF BIDDER FOR SUPPLY INSTALLATION, IMPLEMENTATION, MAINTENANCE & MANAGEMENT OF NEXTGEN SOC & RELATED SERVICES BID NO: PSB/HO-CISO CELL/2026-27/RFP_01 DATED 09/09/2026 Page 68	7.7 On-cloud proposed solution OEM Responsibilities	Page 8	The solution shall support secure connectivity with the Bank's on-premises infrastructure,cloud environments, and external systems through private and secure communication mechanisms.	SIEM is a SaaS solution accessible over the internet using passwords and multi-factor authentication and Https. However, access to your Cortex XSIAM tenant can be restricted based on your Bank's static public IP addresses. Kinkdy change this clause to "" The solution shall support secure connectivity with the Bank's on-premises infrastructure,cloud environments, and external systems through private or secure communication mechanisms via internet or tenant can be restricted based on Bank's static public IP addresses..""	Please refer the addendum for revised clause
1374	RFP Pg 33	Section 7.2.3 Deployment Model Definition		CSP-hosted components shall provide cloud-native High Availability (HA), geographic resiliency and DR in accordance with the SLA, RTO and RPO requirements specified in this RFP.	Cortex XSIAM is pure SaaS Solution hence this clause is not applicable. kindly remove this for SaaS offerings.	Please refer addendum for the revised deployment architecture
1375	RFP Pg 41	7.3.1.1 Modules, Architecture & Deployment:	Point 7	All SIEM components, including collectors, ingestion nodes, correlation engines, processing nodes, etc., are deployed in the prescribed HA architecture irrespective of whether they are deployed at the Bank's Data Centre (DC), Disaster Recovery (DR) Centre, CSP Primary Site, or CSP Secondary Site.	Not applicable, as Cortex XSIAM is a SaaS solution. However, the on-premises Cortex Broker VM component can be deployed in a High Availability (HA) configuration across primary Data Center (DC) and Disaster Recovery (DR) sites	For SaaS-based components, the applicable SaaS SLA shall specify the required uptime/availability commitment. For components deployed at the Bank's DC/DR, the prescribed HA architecture shall apply as specified in the RFP
1376	RFP Pg 43	7.3.2.2 Key Deliverables	Point 7	Backup, retention, restoration, documentation and knowledge transfer for configured security automation capabilities and use cases.	Need more clarification on this clause	No Change, Please be guided by the RFP Refer Section7.2.4.3 Storage and other Requirement
1377	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 2-11	Cloud CSP	3	The proposed cloud infrastructure should be deployed in High Availability mode (N+N) at both primary site and secondary site.	This clause is applicable only if the solution delivered via PaaS, Cortex XSIAM is pure SaaS Solution hence this clause is not applicable. Request you to change the clause "" The cloud infrastructure should have presence in at least 2 cities in India in different SEISMIC Zone OR Deliver 99.99 % uptime from a single cloud region ""	Please refer addendum for the revised clause
1378	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 2-11	Cloud CSP	4	The solution shall meet Bank-defined RPO/RTO and resilience requirements irrespective of the replication technology adopted.	This clause is applicable only if the solution delivered via PaaS, Since Cortex XSIAM is pure SaaS Solution Bank defined RTO RTO will not be applicable.	Please refer addendum for the revised clause
1379	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 2-11	Cloud CSP	10	OEM shall esnure compliance of the complete proposed solution & platform with RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and all applicable regulations throughout the contract period.	Kindly chage is to "" OEM shall esnure compliance of the complete proposed solution & platform with RBI, CERT-In, CSCRF,, IT Act, MeitY and all applicable regulations throughout the contract period.""	Please refer addendum for revised clause
1380	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 2-11	Cloud CSP	16	Solution provider should have capability to provide Alerts & Monitoring interface. Solution should support Remote Administration for administrators	This clause is applicable only if the solution delivered via PaaS, Cortex XSIAM is pure SaaS Solution hence this clause is not applicable. kindly remove this for SaaS offerings.	Please refer addendum for the revised clause
1381	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 2-11	Cloud CSP	18	The cloud infrastructure should have presence in at least 2 cities in India in different SEISMIC Zone	This clause is applicable only if the solution delivered via PaaS, Cortex XSIAM is pure SaaS Solution hence this clause is not applicable. Request you to change ths clause "" The cloud infrastructure should have presence in at least 2 cities in India in different SEISMIC Zone OR Deliver 99.99 % uptime from a single cloud region ""	Please refer addendum for the revised clause
1382	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 2-11	Cloud CSP	163	The solution should be deployed on dedicated cloud instance for Bank. The Bidder shall finalize the cloud solution requirement in line with volume, request/response times, cloud replication requirements, back up disk & media based.	Kinldy chnage this clause to ""The solution should be deployed on dedicated cloud instance for Bank. The Bidder shall finalize the cloud solution requirement in line with volume, request/response times, cloud replication requirements""	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1383	Appendix 1A Page 40	NDR Functional Compliance Sheet	Clause 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high- availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	The Clause mandates Cloud based SaaS model, while RFP Page 30, Page 35, section 7.2.4.1 clause 'd' asks for on Premesis solution "The NDR shall be deployed On-Premises". We request to modify the clause to include On-Prem solution. Justification: To include solutions which are on-Prem based	Please refer Addendum for revised clause
1384	Appendix 1A Page 40	NDR Functional Compliance Sheet	Clause 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high- availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	The Clause asks for Active-Active HA architecture, we request to include Active-Standby Mode. Justification: Management Console is central console, it cannot be deployed in Active-Active mode, as it is a central component.	Please refer Addendum for revised clause
1385	Appendix 1A Page 41	NDR Functional Compliance Sheet	Clause 18	Solution should have the capabilities to create and run security playbooks for automation and better MTTD/MTTR on the basis of criticality of threat/server	Proposed solution adopts below appraoch for automated MTTD, Solution need investigative workflows and all the alerts need to be validated before building any Active Response Solution is having inbuilt playbooks like Host, Session and Packet analysis. once alert is validated Active Response can be triggered. Hope the approach is acceptable	Yes, your understanding is correct Also, Please refer addendum for the revised clause
1386	Page 66	7.6.7	Training	At a minimum, the following training programs shall be conducted for each proposed solution / OEM appointed officials: Duration per Session and Munimum Number of Sessions	Overall there is a requirement of 15 Sessions and Duration per session is 2 or 3 days. This takes the total training per solution to 40 days. This is very large reqirement of training, we request to make it to 3 days for NDR solution	Please refer addendum for revised clause
1387	Page 63	7.6.6	Testing, clause 3	The bidder shall provision and maintain dedicated Development, Testing, UAT, and Pre-Production environments throughout the contract period.	Is UAT Environment required for NDR solution also, given that NDR is a Passive and out of path solution.	Please refer addendum for revised clause
1388	30	7.2.1 Solutions – Master Deployment Matrix	#8. Vulnerability assessment (VA) & vulnerability lifecycle management	Bank Location: Standalone at DC and Standalone at DR. Management Console: Deployed at both DC and DR	As per this RFP Technical Specification of VA & VLM,document #1788963129, #12 "The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and failover capabilities" where the 7.2.1 of suggests standalone deployment at DC, DR and console availablity at both DC and DR. These two partially contradict each other. We request you to kindly confirm if standalone VA & VM in DC and DR are expected to function independently. Maintaining two standalone environments with both consoles accessibility will lead to duplication of vulnerabilities, configuration efforts and it will cost upto 2X in terms of licensing. Though its not clear but we assume that you need one VM in DC and one in DR where primary one shares configuration backup on secondary and secondary can take over when the primary goes down, the primary VM solution should be able to scan both the DCs and vice-versa. If this understanding is correct, kindly update the clause as following - 'The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and active-cold standby failover capabilities where only one active console shall be accessible at a time'.	No Change, Please be guided by the RFP
1389	260	16.21.2 Volumetrics-Solution-wise Requirements	10 Vulnerability Assessment & Management (VA-VM) Minimum Numbers of IPs: 4000	10 Vulnerability Assessment & Management (VA-VM) Minimum Numbers of IPs: 4000	As per the RFP #1788963158, page 257 16.21.1 Current IT assets, P&SB has 2500 servers, 300 DB, 200 Apps, 12000 endpoints/desktops and 7200 routers and switches whereas the VA/VM IP coverage is mention as "Minimum" 4000. We seek your guidance and confirmation on the final count of assets/IPs you need coverage from day #1, given "minimum" count may lead to each bidder proposing seperate numbers and very likely excluding important assets from highly important VA & VM exercise. Without a defined and finite asset count, bidders cannot be compared on a like-for-like basis as the ones concerned about the VA/VM security posture of the infra will propose to cover more IPs/Assets while some may cover bare minimum and appear more competitive. We request you to kindly provide the final IP count required for VA/VM from day #1 considering the licenses are bound to assets and deleting the asset will delete all historic vulnerability and trends data, deleted asset will not cover alerts, ITSM integration and cannot be considered as part of VM exercise. As per the CERT'in recommendations (https://www.cert-in.org.in/PDF/guidelinesgovtentities.pdf) as well as industry best practices, entire ICT infrastructure should be part of the vulnerability management exercise and network device inclusion is absolute must given these are critical assets and in some zones exposed directly to internet.	No Change, Please be guided by the RFP
1390	38	On premises deployment of solutions	Storage Capacity & Sizing	• The Bidder shall provide detailed storage sizing based on expected data/log volumes, peak ingestion rate, retention period, indexing, enrichment, compression, replication, backup, archival and anticipated annual growth. Adequate capacity shall be provisioned for the complete contract period.	As per the RFP #1788963158, storage duration on the primary storage of the solution itself is mention for Cloud/SaaS/Hybrid to be 3 months, same is not clearly specified for VA & VM. Kindly confirm how long should the VA & VM solution retain the asset, vulnerability, logs, activities, historic trend etc. As per CERT-IN it must be 6 months. Kindly confirm if you wish the solution to retain this info on its own primary storage to be for 6 months or less.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1391	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - VA-VM	VA-VM S.No. 9	Each scanning engine shall support web application security assessment together with traditional infrastructure vulnerability and configuration/compliance assessment. The solution shall identify vulnerabilities, missing patches, insecure configurations, and compliance deviations, and generate comprehensive reports containing risk severity, evidence of findings, affected assets, and remediation recommendations to support security governance, audit, and regulatory compliance.	While its possible to perform this via VA VM solution with additional WAS/DAST license, this will be a duplication of solution given you are already asking for seperate 'Application Security Testing Tool'. Hence, we request you to kindly move the 'Web application security assessment' from VA & VM requirements to DAST as this is a DAST requirement and may unnecessorily require to duplicate the licenses, solution and hardware.	No Change, Please be guided by the RFP
1392	Functional Compliance Sheet pp.48-51 (Appendix 1A)	Appendix 1A - VA-VM	VA-VM S.No. 36-52 and S.No. 61-77; S.No. 87 and S.No. 89	All technical compliances of VA-VM S.No. 36-52 and S.No. 61-77; S.No. 87 and S.No. 89	S.N 61-77 are likely duplicates of S.N 36 to 52 with minor changes. Request you to kindly review and confirm if this is intentional or typo. If not intentional, kindly remove duplicates to have the score calculated accordingly.	No Change, Please be guided by the RFP
1393	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 12	The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and failover capabilities.	VM solution is not an inline and always active solution.VM solutions across the industry do not have failovers similar to inline solutions such as firewalls. Hence, we request you to kindly consider the failover scenario as active - cold standby with documented backup-restore and a controlled switchover in place of automatic console failover. We request you to kindly update the clause as - The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and failover capabilities either automatically or using manual and controlled backup restore.	No Change, Please be guided by the RFP
1394	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 15	The proposed solution shall support integration with SIEM, SOAR, Threat Intelligence Platforms, NAC, and other security platforms through APIs or standard integration mechanisms.	Kindly share details (Vendor/Model/Version) of the SIEM, SOAR, TIP and NAC solution you would want to integrate with for us to identify the availablity of standard or API based integration and accordingly finalize the deployment efforts.	No Change, Please be guided by the RFP
1395	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 16	The proposed solution shall integrate with Privileged Access Management (PAM) solutions for secure credential management during authenticated scans.	Kindly share details (Vendor/Model/Version) of the PAM solution you would want to integrate with for us to identify the availablity of integration and also identify the deployment efforts.	Bank is currently procuring PAM solution through separate RFP.
1396	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 17	The proposed solution shall integrate with IT Service Management (ITSM) and ticketing platforms for automated vulnerability tracking and remediation workflows.	Kindly share details (Vendor/Model/Version) of the ITSM solution you would want to integrate with for us to identify the availablity of standard or API based integration and accordingly finalize the deployment efforts.	ITSM - Manage Engine
1397	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 29	The proposed solution shall support vulnerability assessment and compliance reporting aligned with PCI DSS requirements.	We request you to kindly confirm whether you only require to perform PCI DSS internal scanning and reporting on-premises or you also require the PCI- ASV attestation. If Attestation is required, kindly share the exact asset count for which the attestation is needed and how many attestations are to be submitted within 1 year.	No Change, Please be guided by the RFP
1398	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 42	The solution shall support vulnerability assessment of VMware ESXi, Hyper-V, Nutanix AHV, Kubernetes, OpenShift and container platforms.	We request you to kindly confirm whether you need the OS and platform vulnerability assessment of these container solutions or you need a comprehensive container security solution with the ability to identity vulnerabilities of images, registries and their components. If you need comprehensive container security assessment, we request you to kinly move this required to CNAPP solution as its usually part of cloud security solutions and not VM solution.	No Change, Please be guided by the RFP
1399	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 45	The solution shall integrate with enterprise CMDB, ITSM, SIEM, SOAR, PAM and NAC platforms through secure REST APIs.	Kindly share details (Vendor/Model/Version) of the required solutions you would want to integrate with for us to identify the deployment efforts.	Please refer addendum for the revised clause Details shall be shared with successful bidder
1400	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 47	The solution shall support Multi-Factor Authentication (MFA), LDAP, Active Directory, SAML 2.0 and OpenID Connect authentication.	We request you to kindly remove the OpenID and update the clause as following - The solution shall support Multi-Factor Authentication (MFA via SAML and/or LDAP), LDAP, Active Directory, SAML 2.0.	No Change, Please be guided by the RFP
1401	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 48	The solution shall support secure encrypted communication using TLS 1.3 and cryptographic modules compliant with FIPS 140-3 or equivalent internationally recognized standards.	We request you to kindly allow the FIPS 140-2 or equivilent solution transitioning to FIPS 140-3 to participate and update the clause as following - The solution shall support secure encrypted communication using TLS 1.3 and cryptographic modules compliant with FIPS 140-2 or FIPS 140-3 or equivalent internationally recognized standards.	Please refer addendum for revised clause
1402	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 51	The solution shall identify internet-facing assets and continuously monitor externally exposed services.	We request you to kindly remove this clause as its an ASM(Attack Surface Management) requirements which is already asked separate service based solution of the RFP.	Please refer the addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1403	Functional Compliance Sheet p.49 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 56	The solution shall support digitally signed and password-protected reports with configurable retention and archival.	We request you to kindly update the clause as following - The solution shall support password-protected reports with configurable retention and archival.	Please refer addendum for revised clause
1404	Functional Compliance Sheet p.49 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 60	The solution shall provide comprehensive REST APIs and webhook support for automation and integration with enterprise security platforms.	We request you to kindly update the clause as following - The solution shall provide comprehensive REST APIs or webhook support for automation and integration with enterprise security platforms.	Please refer addendum for revised clause
1405	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 87	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	We request you to kindly remove this clause from VM VM and move it to CTEM as this is a CTEM requirement, a solution that can be cloud/SaaS based. Given the data soveraginity and sensitivity of bank's vulnerabilities data, the platform is correctly requested to be on-prem which shall also be able to function without any internet connectivity. Hence, AI powering the on-prem application to achieve all the listed items is not viable. We request you to kindly remove this point and move it to CTEM.	Please refer the addendum for revised clause
1406	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 88	Unified, correlated findings intelligence. Every scanning engine — across web, API, network and host, cloud, containers, mobile, source code, device configuration and identity — reports into a single normalized findings model..	This is a CTEM requirement as VM solution won't perform VA of source code, identity etc. Kindly move this from VA VM to CTEM requirements.	No Change, Please be guided by the RFP
1407	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 89	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	This is a duplicate of S.N. #87, kindly remove it.	Please refer the addendum for revised clause
1408	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 90	Mobile Application Security Testing: The proposed solution shall support static security analysis of Android and iOS mobile application packages, including APK/AAB and IPA formats, and shall provide security assessment mapped to recognized mobile application security standards and methodologies such as OWASP MASVS and MASTG.	This is not part of any VA/VM solution in industry and belongs to application security testing. We request you to kindly move this to 'Application Security Testing Tool'.	No Change, Please be guided by the RFP
1409	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 91	White-Label Reporting and Approval Workflow: The proposed solution shall support customizable/white-label security assessment reports, including organization-specific branding and configurable report content. The solution shall support role-based maker-checker workflow for report generation, review, approval, and controlled release of finalized reports.	We request you to kindly update the clause as following - White-Label Reporting and Approval Workflow: The proposed solution shall support customizable/white-label security assessment reports, including organization-specific branding and configurable report content. The solution shall support role-based access for report generation, review of the finalized reports.	Please refer the addendum for revised clause
1410	92	7.18.1 Compute Infrastructure	10. Non-production:	10. Non-production: a) The non-production environments should have the same software and hardware setup as deployed in production environments meeting all RFP requirements.	While this clause suggests the hardware and software setup of non-prod to be same, "16.21 Annexure 21: Sizing/Volumetrics, Data Retention and Current Infrastructure" suggests the VM based solution to have minimum 10% size. Kindly confirm if the 10% requirement of non-production infra is for only licenses whereas the hardware specs are to be identical to prod or both the licenses as well as hardware/software specs to be 10% of the production infra. Also kindly confirm if the non-production is to be setup only at DC or DC as well as DR.	Please refer addendum for the revised clause
1411	Functional Compliance Sheet pp.47-51 (Appendix 1A)	Appendix 1A - VA-VM	TOTAL MARKS row and S.No. 1 to 94	TOTAL MARKS - 850	While the VA-VM section contains 94 scoreable clauses, each carrying Maximum Marks of 10, which totals 940 marks, whereas the TOTAL MARKS row of the section states 850. We request you to kindly publish the corrected total and confirm the marks allocated per clause, so that bidders can compute the Respective Solution Compliance required by the Appendix 1A summary sheet consistently.	Please refer addendum for the revised clause
1412	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 19, 20, 43 and 44 (missing) and TOTAL MARKS row	CNAPP section is numbered from S.No. 1 to S.No. 60; however S.No. 19, 20, 43 and 44 do not appear in the sheet. TOTAL MARKS - 560.	The CNAPP section is numbered up to S.No. 60 but S.No. 19, 20, 43 and 44 are not present, leaving 56 scoreable clauses which, at 10 marks each, reconciles to the stated TOTAL MARKS of 560. We request you to kindly confirm whether these four clauses have been intentionally deleted or have been inadvertently omitted from the published sheet. If clauses exist against these serial numbers, kindly publish them along with the revised TOTAL MARKS; if they have been deleted, kindly re-issue the sheet with continuous numbering so that bidders' compliance responses and score computation remain traceable to the Bank's evaluation sheet.	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1413	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 16	The solution shall support integration with relevant source-code repositories, development tools, build systems, CI/CD platforms and security workflows, either natively or through supported connectors/APIs.	A CNAPP integrates with source-code repositories and CI/CD platforms for Infrastructure-as-Code (IaC), container image and cloud-configuration assessment. It does not act as a source-code security testing tool, which is the function of the separately procured 'Application Security Testing Tool' in this RFP. We request you to kindly update the clause as following - "The solution shall support integration with relevant source-code repositories, development tools, build systems, CI/CD platforms and security workflows, either natively or through supported connectors/APIs, for the purpose of Infrastructure-as-Code, container image and cloud configuration assessment."	No Change, Please be guided by the RFP
1414	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 17 and S.No. 18	S.No. 17 - The solution shall identify security risks and known vulnerabilities associated with third-party, open-source and externally sourced software components and dependencies used by cloud-native applications. S.No. 18 - The solution shall provide visibility into application dependencies and software components and shall identify affected applications where a vulnerable component or dependency is detected.	Identification of third-party/open-source components and application dependencies is a Software Composition Analysis (SCA)/SBOM capability which belongs to the 'Application Security Testing Tool' scope already sought separately in this RFP, and requiring it again under CNAPP will lead to duplication of licences and cost without additional security benefit to the Bank. We request you to kindly either move these clauses to the Application Security Testing Tool requirements, or update them as following - "The solution shall identify known vulnerabilities in third-party and open-source software components and dependencies present within container images, registries and cloud workloads assessed by the platform, and shall identify the affected cloud-native applications/components."	No Change, Please be guided by the RFP
1415	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 24	The solution shall provide security visibility for cloud-native APIs and application interfaces, including risks related to exposure, authentication, authorization, access control and relevant configurations, where supported.	Discovery and security assessment of application APIs (including authentication/authorization testing of API endpoints) is the function of a dedicated API Security/API posture solution, and is not a native capability of CNAPP platforms. CNAPP platforms provide visibility of cloud-native API gateway and managed API service configurations and their exposure. We request you to kindly update the clause as following - "The solution shall provide security visibility for cloud-provider API gateway/managed API services and application interfaces discovered from the cloud control plane, including risks related to public exposure, authentication/authorization configuration and access control settings, where supported by the respective cloud platform."	No Change, Please be guided by the RFP
1416	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 26	The solution shall provide visibility into application access to sensitive or critical data and identify security risks arising from inappropriate application access, exposure or relationships, where supported.	As worded, this clause can be read as requiring full Data Security Posture Management (DSPM) with data discovery and classification of the Bank's data stores, which is a separately licensable product category and is not part of a baseline CNAPP. We request you to kindly confirm whether DSPM (data discovery and classification) is intended to be in scope of the CNAPP. If it is not intended, we request you to kindly update the clause as following - "The solution shall provide visibility into application and identity access paths to cloud data stores and shall identify security risks arising from public exposure, excessive access or inappropriate relationships to such data stores, where supported by the respective cloud platform." If DSPM is intended, kindly publish the applicable volumetrics (number/size of data stores) so that bidders can size and price the module consistently.	No Change, Please be guided by the RFP
1417	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 27	The solution shall identify vulnerable application components that are reachable, exposed or potentially exploitable within the application's dependency or relationship graph, where such analysis is supported.	Code-level 'reachability' analysis of a vulnerable function within an application's dependency graph is an SCA/ASPM capability delivered by application security testing tools. CNAPP platforms determine exposure and exploitability from cloud context - internet exposure, network path, identity privilege and attack-path relationships. We request you to kindly update the clause as following - "The solution shall identify vulnerable application components that are internet-exposed, network-reachable or potentially exploitable based on cloud exposure, network path, identity privilege and attack-path relationship analysis, where such analysis is supported by the proposed solution."	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1418	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 32	The solution shall provide guided, semi-automated and/or automated remediation capabilities for supported application-security findings.	Fully automated remediation executed directly by a security platform on a production banking cloud environment is generally not permitted under change-management controls, and CNAPP platforms deliver remediation as guided steps and auto-generated remediation artefacts (e.g., IaC fix code/pull requests, CLI commands, policy snippets) which are then applied by the Bank/implementation partner through the Bank's change process. We request you to kindly update the clause as following - "The solution shall provide guided remediation and automatically generated remediation artefacts (such as IaC remediation code, pull requests, CLI commands or policy snippets) for supported application-security findings, which may be applied through the Bank's approved change-management process or through integration with the Bank's SOAR/ITSM platform."	No Change, Please be guided by the RFP
1419	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 59	The solution shall support high availability and service continuity appropriate to the proposed deployment architecture and shall provide mechanisms for recovery of relevant configurations, policies and security information.	Where the CNAPP is delivered as OEM-managed SaaS, high availability, redundancy, backup and disaster recovery are provided by the OEM within the platform and are governed by the OEM's published availability SLA; the Bank cannot be provided Bank-operated HA/DR or restore mechanisms for a SaaS platform. We request you to kindly update the clause as following - "For SaaS-delivered solutions, the OEM shall provide high availability, redundancy and disaster recovery within the platform in line with its published availability SLA, and shall provide mechanisms for export/retrieval of relevant configurations, policies and security information. For on-premises components, if any, the solution shall support HA and documented backup-restore."	Please refer the addendum for revised clause
1420	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP - Section scope (S.No. 1 to 50, principally S.No. 1, 6, 7, 8 to 41)	The proposed Cloud Workload Protection Platform (CWPP) shall provide centralized capabilities for protecting, monitoring, detecting, investigating and responding to security threats affecting cloud workloads during runtime. (S.No. 1) and the runtime detection, prevention, response, forensics and threat-hunting clauses at S.No. 6 to 41.	The CWPP section as drafted is predominantly a runtime endpoint/server threat prevention, detection and response (EDR/XDR-class) specification - in-guest malware and ransomware prevention, exploit prevention, host IDS/IPS, file integrity monitoring, process and command-line telemetry, containment actions such as process termination, file quarantine and workload isolation, forensic timelines, process trees and threat hunting. These are delivered by an EDR/XDR agent platform, whereas the CNAPP/CWPP category referenced elsewhere in this RFP delivers agentless workload vulnerability, malware, misconfiguration, identity, secrets and exposure assessment with attack-path context. Given the Bank is separately procuring EDR/XDR and SOC/SIEM capabilities under this very RFP, we request you to kindly clarify and confirm any one of the following, so that bidders are not compelled to bid a second endpoint agent on the same servers: 1. That runtime prevention, containment and forensics requirements of the CWPP section may be met through the Bank's in-scope EDR/XDR platform, with the CWPP providing agentless workload exposure assessment, posture and attack-path context integrated with it; or 2. That the CWPP section may be responded to on a multi-OEM/consortium basis with clear identification of the product meeting each clause (consistent with S.No. 50 of this section); or 3. That the runtime prevention/response clauses be moved	No Change, Please be guided by the RFP
1421	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 2 and S.No. 3	S.No. 2 - The solution shall support protection of workloads deployed across physical, virtual, private-cloud, public-cloud and hybrid-cloud environments, as applicable. S.No. 3 - The solution shall support major public-cloud environments including AWS, Microsoft Azure and Google Cloud Platform, as applicable.	CWPP licensing and sizing depend entirely on the workload inventory in scope, and the clause extends coverage to physical and private-cloud workloads in addition to public cloud. We request you to kindly publish, for the CWPP scope, the workload volumetrics for day #1 and for the contract period - number of physical servers, virtual machines, public-cloud instances (per CSP), container hosts/nodes, Kubernetes clusters and serverless functions - along with the CSP accounts/subscriptions/projects in scope. Kindly also confirm which of these environments are mandatory on day #1, since 'as applicable' may lead each bidder to price a different scope and render the commercial bids non-comparable.	No Change, Please be guided by the RFP
1422	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 8, S.No. 21 and S.No. 22	S.No. 8 - The solution shall detect and prevent, where supported, malware, ransomware, trojans, rootkits and other malicious software or activities affecting protected workloads. S.No. 21 - The solution shall provide protection against ransomware and destructive activities, including detection of abnormal file encryption or mass file modification behavior. S.No. 22 - The solution shall provide exploit detection and/or prevention capabilities for supported workload operating systems and applications.	In-guest prevention of malware, ransomware, trojans and rootkits, behavioural detection of mass file-encryption, and memory/exploit prevention require a kernel-level endpoint prevention engine (EDR/EPP) and are not functions of an agentless cloud workload protection platform, which performs malware and vulnerability detection through workload snapshot/disk analysis without in-line blocking. We request you to kindly move these clauses to the EDR/XDR section of the RFP, or update them as following - "The solution shall detect malware, ransomware, trojans, rootkits, malicious files and destructive activity affecting protected workloads through agentless and/or agent-based assessment, and shall support prevention/blocking natively or through integration with the Bank's EDR/XDR platform."	S.No. 8- No Change, Please be guided by the RFP S.No. 21- No Change, Please be guided by the RFP S.No. 22- No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1423	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 9 to S.No. 14	S.No. 9 to 14 - monitoring of process execution and process behaviour; detection of suspicious process chains and abnormal parent-child relationships; monitoring of command-line execution, scripts and interpreters; detection of Living-off-the-Land techniques; behavioural/heuristic analysis of anomalous activity; and detection of privilege escalation, persistence, lateral movement and credential misuse.	These clauses describe in-guest runtime behavioural telemetry (process, command-line, script and parent-child process monitoring) which is collected by an EDR/XDR sensor and analysed in the SOC/SIEM. A CWPP that assesses workload exposure agentlessly does not generate kernel-level process telemetry. We request you to kindly move these clauses to the EDR/XDR section, or update them as following - "The solution shall provide the specified runtime behavioural detection capabilities natively or through correlation of telemetry from the Bank's EDR/XDR and SIEM platforms, and shall enrich such detections with workload vulnerability, identity, configuration and exposure context." Kindly also confirm that a capability delivered through such integration will not be treated as non-compliant, consistent with the principle already accepted at CNAPP S.No. 53 of this Appendix.	No Change, Please be guided by the RFP
1424	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 15, S.No. 16 and S.No. 17	S.No. 15 - The solution shall monitor relevant network communications involving protected workloads and identify suspicious or unauthorized communication patterns. S.No. 16 - The solution shall identify communication with known or suspected malicious infrastructure, including malicious IP addresses, domains, URLs, command-and-control infrastructure or equivalent threat indicators, where applicable. S.No. 17 - The solution shall provide host/workload-based intrusion detection and/or prevention capabilities for supported operating systems and workloads.	Host-based intrusion detection/prevention and in-line inspection of workload network traffic for command-and-control communication are functions of HIDS/HIPS agents, NDR and NGFW/IPS controls, all of which are separately in scope in this RFP. A CWPP provides network exposure and reachability analysis from cloud configuration (security groups, NACLs, routes, load balancers, public exposure) rather than packet-level inspection. We request you to kindly move these clauses to the EDR/XDR, NDR or NGFW sections as appropriate, or update them as following - "The solution shall identify workload network exposure, reachable paths and unauthorized/high-risk communication paths from cloud network configuration and available flow logs, and shall support identification of communication with known malicious infrastructure natively or through integration with the Bank's EDR/XDR, NDR, NGFW and SIEM platforms."	S.No. 15- No Change, Please be guided by the RFP S.No. 16- No Change, Please be guided by the RFP S.No. 17- No Change, Please be guided by the RFP
1425	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 18 and S.No. 19	S.No. 18 - The solution shall monitor critical files, directories, system objects and configuration elements for unauthorized modification, creation or deletion, where supported. S.No. 19 - The solution shall provide file integrity monitoring for designated critical files, directories and system objects.	File Integrity Monitoring (FIM) requires a resident agent performing real-time file-system event monitoring on the workload and is a standard EDR/host-integrity capability. It is not delivered by an agentless cloud workload protection platform. We request you to kindly move these clauses to the EDR/XDR section, or update them as following - "File integrity monitoring for designated critical files, directories and system objects shall be provided natively or through integration with the Bank's EDR/XDR or host-integrity solution, with the resulting events available for correlation and reporting."	No Change, Please be guided by the RFP
1426	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 20 and S.No. 24	S.No. 20 - The solution shall detect suspicious creation or modification of system accounts, services, scheduled tasks and other persistence mechanisms, where applicable. S.No. 24 - The solution shall support detection and/or prevention of web-shell and other unauthorized application-level persistence mechanisms, where applicable.	Real-time detection of persistence mechanisms and prevention of web-shell execution are runtime endpoint and web application protection (EDR/WAF) functions. A CWPP can identify such artefacts through periodic workload assessment but cannot prevent their execution. We request you to kindly move these clauses to the EDR/XDR and WAF sections respectively, or update them as following - "The solution shall identify unauthorized accounts, services, scheduled tasks, web-shells and other persistence artefacts present on assessed workloads, and shall support real-time detection/prevention natively or through integration with the Bank's EDR/XDR and WAF platforms."	No Change, Please be guided by the RFP
1427	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 23	The solution shall support virtual patching or equivalent compensating protection mechanisms, where applicable, for vulnerabilities for which immediate patching is not feasible.	Virtual patching is enforced by in-line controls - host IPS agents, NGFW/IPS and WAF - all of which are separately procured under this RFP. A workload protection/exposure platform identifies the vulnerability and recommends the compensating control; it does not itself enforce a virtual patch. We request you to kindly remove this clause from the CWPP section as it is already covered by the Bank's NGFW/IPS and WAF requirements, or update it as following - "For vulnerabilities where immediate patching is not feasible, the solution shall identify the exposure, provide risk context and recommend applicable compensating controls, which may be enforced through the Bank's in-line security controls (host IPS, NGFW/IPS, WAF) through supported integration."	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1428	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 25, 26, 27 and 28	S.No. 25 - runtime security monitoring and threat detection for containerized workloads; S.No. 26 - runtime protection for Kubernetes workloads including pods, containers and workload processes; S.No. 27 - detection of suspicious behaviour involving containers, pods, workload processes and workload-to-workload communications; S.No. 28 - security monitoring for serverless workloads/functions.	Container and Kubernetes runtime protection requires a privileged runtime sensor (e.g., eBPF/DaemonSet-based) on every node, which materially differs from the container and Kubernetes security posture, image/registry scanning, admission control and Kubernetes misconfiguration and RBAC assessment delivered by a CNAPP/CWPP. We request you to kindly clarify whether the Bank requires (a) container/Kubernetes runtime sensor-based prevention or (b) container and Kubernetes security posture with image, registry, IaC, admission-control and RBAC assessment plus runtime detection through the Bank's EDR/XDR on the worker nodes. We request you to kindly permit option (b) and update the clauses to allow the capability to be delivered through posture assessment, admission control and integration with the Bank's EDR/XDR and SIEM, failing which the clause is restrictive to a small subset of OEMs. Kindly also publish the number of Kubernetes clusters, nodes and serverless functions in scope for sizing.	No Change, Please be guided by the RFP
1429	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 29 and S.No. 30	S.No. 29 - The solution shall support agent-based and/or agentless protection mechanisms, as applicable to different workload types and supported environments. S.No. 30 - Where an agent is required, the solution shall provide mechanisms for secure deployment, centralized management, health monitoring and controlled upgrade of the workload protection agent.	We note and appreciate that S.No. 29 permits agentless mechanisms. However, several other clauses in this section (S.No. 8 to 41) are achievable only through an in-guest agent, which contradicts the option provided in S.No. 29. We request you to kindly confirm that an agentless-first architecture, supplemented where required by the Bank's EDR/XDR agent already deployed on the workloads, will be accepted as compliant against this section, and that S.No. 30 shall apply only where the bidder proposes its own agent. Kindly also confirm that no additional agent is mandated on workloads that already carry the Bank's EDR/XDR agent, in view of performance and change-management impact on production banking workloads.	No Change, Please be guided by the RFP
1430	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 32 and S.No. 33	S.No. 32 - The solution shall support configurable response actions for detected threats, including alerting, blocking, process termination, file quarantine, workload isolation or other equivalent containment actions, as applicable. S.No. 33 - The solution shall provide workload isolation or containment capabilities to limit the impact or spread of a confirmed or suspected compromise, where supported.	Process termination, file quarantine and host/network isolation are kernel-level containment actions performed by an EDR/XDR agent. An agentless workload protection platform performs cloud-control-plane actions (such as snapshotting, tagging, security-group/identity restriction) and orchestrates containment through the Bank's EDR/XDR and SOAR. We request you to kindly move these clauses to the EDR/XDR section, or update them as following - "The solution shall support configurable response actions for detected threats, including alerting, notification, cloud-control-plane containment actions (such as network/identity restriction, snapshot and tagging) natively, and process termination, file quarantine and workload isolation through integration with the Bank's EDR/XDR and SOAR platforms."	S.No. 32 - No Change, Please be guided by the RFP S.No. 33 - No Change, Please be guided by the RFP
1431	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 34, 35, 36 and 37	S.No. 34 - security investigation using process, file, network, user, workload and event-level information; S.No. 35 - historical workload activity and security-event information sufficient for investigation and forensic analysis; S.No. 36 - process-tree or equivalent process-relationship visualization; S.No. 37 - workload-level threat hunting using available security telemetry and configurable search criteria.	Retention of process/file/network event-level telemetry, process-tree reconstruction and telemetry-based threat hunting are EDR/XDR and SIEM functions and require an in-guest sensor. Additionally, these clauses do not specify a retention period, which makes consistent sizing and pricing impossible. We request you to kindly (a) move these clauses to the EDR/XDR and SIEM sections or permit compliance through integration with the Bank's EDR/XDR and SIEM platforms, and (b) if retained under CWPP, publish the mandated telemetry retention period (hot/warm/archive) and the expected daily event volume per workload, so that all bidders size storage and licences on a common basis.	No Change, Please be guided by the RFP
1432	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 38 and S.No. 39	S.No. 38 - The solution shall support identification and searching of Indicators of Compromise (IoCs), including supported hashes, IP addresses, domains, URLs and equivalent indicators. S.No. 39 - The solution shall support integration with external threat-intelligence sources to enhance workload threat detection and investigation.	Retrospective and real-time IoC sweeps across workloads are performed on EDR/XDR telemetry or in the SIEM, where the Bank's threat-intelligence platform feeds are already consolidated under this RFP. We request you to kindly update the clauses as following - "The solution shall support identification and searching of Indicators of Compromise (hashes, IP addresses, domains, URLs and equivalent indicators) against available workload assessment data natively, and across workload runtime telemetry through integration with the Bank's EDR/XDR, SIEM and threat-intelligence platforms. The solution shall support ingestion of external threat-intelligence to enrich and prioritise workload findings."	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1433	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 47 and S.No. 48	S.No. 47 - The solution shall support high availability and service continuity appropriate to the proposed deployment architecture and shall provide mechanisms for recovery of relevant configurations and security policies. S.No. 48 - The solution shall provide mechanisms to identify the protection health/status of onboarded workloads, including agent, connector or communication health where applicable.	For OEM-managed SaaS delivery, high availability, redundancy and disaster recovery are provided within the OEM platform under its published availability SLA and cannot be operated or restored by the Bank. We request you to kindly update S.No. 47 as following - "For SaaS-delivered solutions, the OEM shall provide high availability, redundancy and disaster recovery within the platform in line with its published availability SLA and shall provide mechanisms for export/retrieval of relevant configurations and security policies. For on-premises components, if any, the solution shall support HA and documented backup-restore." For S.No. 48, we request confirmation that reporting of connector/cloud-account onboarding and assessment health (and agent health only where an agent is proposed) shall be treated as compliant.	Please refer the addendum for revised clause
1434	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 49	The solution shall support consumption and correlation of relevant vulnerability, SBOM, CBOM and threat-intelligence information from the Bank's separately procured security solutions through APIs, supported integrations or equivalent mechanisms, where technically supported.	Consumption of Cryptographic Bill of Materials (CBOM) is an emerging requirement with no single established interchange standard, and correlation is only feasible if the source system and format are known. We request you to kindly confirm (a) the source solutions and the exact formats/standards in which SBOM and CBOM will be provided by the Bank (e.g., CycloneDX, SPDX and version), and (b) that where a standard format/API is not made available by the source solution, non-availability of such correlation shall not be treated as non-compliance, consistent with the qualifier 'where technically supported' in the clause.	No Change, Please be guided by the RFP
1435	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM - Section scope (S.No. 1 to 69 and TOTAL MARKS 690)	Continuous Threat Exposure Management (CTEM) - all functional specifications, S.No. 1 to 69, TOTAL MARKS 690.	A significant proportion of the CTEM section (illustratively S.No. 1, 2, 5, 7 to 13, 18 to 23, 35, 55, 56, 57 and 67) specifies Cyber Threat Intelligence (CTI) and Digital Risk Protection (DRP) service deliverables - multilingual dark-web collection and translation, analyst-authored periodic and ad-hoc research reports, VIP investigation reports, threat-actor dossiers and engagement with threat actors, compromised-credential and payment-card monitoring, takedown/reporting to external authorities, named analyst and incident-response services. These are analyst-delivered managed services and are distinct from a Continuous Threat Exposure Management platform, which (per the recognised CTEM framework) delivers scoping, discovery, prioritisation, validation and mobilisation of exposures across the attack surface. As currently drafted, the section can be fully met only by DRP/CTI service providers and is restrictive to exposure-management platform OEMs, even though the Bank has separately (at VA-VM S.No. 87 and 88) contemplated CTEM as the platform that consolidates and prioritises findings across scanning engines. We therefore request you to kindly split this section into (a) 'CTEM / Exposure Management Platform' and (b) 'Cyber Threat Intelligence and Digital Risk Protection Services', with separate functional specifications, separate marks and separate	No Change, Please be guided by the RFP
1436	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 1, S.No. 2 and S.No. 7	S.No. 1 - The solution should collect intelligence from multiple languages and relevant regional sources, with support for multilingual threat intelligence processing and analysis. S.No. 2 - The solution should support translation or interpretation of collected intelligence into English. S.No. 7 - Each intelligence item should include metadata such as date, author, source, and pre-classification of raw data.	Multilingual collection from closed/regional sources, machine translation of collected raw intelligence, and 'author'-level metadata with pre-classification of raw data are characteristics of a dark-web/DRP collection platform and are not features of a CTEM/exposure management platform. We request you to kindly move these clauses to the proposed Cyber Threat Intelligence/DRP service scope. If they are retained under CTEM, we request you to kindly update them as following - "The solution shall provide vulnerability, exploit and exposure intelligence in English, with source, publication date and classification metadata, and shall support ingestion of multilingual/regional intelligence from bank-approved third-party sources through supported integration mechanisms."	Please refer the addendum for revised clause
1437	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 8 and S.No. 53	S.No. 8 - The solution should allow messaging and collaboration within the context of a specific intelligence item. S.No. 53 - Each alert should include a discussion board for eligible users to collaborate within the alert context.	An in-product messaging/discussion board is a vendor-specific user-interface feature, and for a bank, collaboration and audit trails on security findings are better retained in the Bank's ITSM/SOAR system of record rather than in a third-party SaaS console. We request you to kindly update the clauses as following - "The solution shall support collaboration on a specific exposure, alert or intelligence item through comments/annotations, assignment and status tracking within the platform and/or through bidirectional integration with the Bank's ITSM/SOAR/ticketing platform."	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1438	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 9	The solution shall provide access to proprietary, internally generated, licensed or equivalent high-quality threat intelligence sources capable of providing actionable intelligence relevant to the Bank's environment.	We request confirmation of the nature of intelligence expected. Exposure-management OEMs provide proprietary research-generated vulnerability, exploit and exposure intelligence (including exploit availability, exploitation-in-the-wild, ransomware association and predictive exploitability), whereas dark-web/actor intelligence is sourced by DRP providers. We request you to kindly update the clause as following - "The solution shall provide access to the OEM's proprietary/internally generated and/or licensed intelligence covering vulnerabilities, exploits, exploitation activity and exposures relevant to the Bank's environment, and shall support ingestion of additional bank-approved third-party intelligence sources."	No Change, Please be guided by the RFP
1439	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 10	Analysts should perform threat hunting activities to find findings outside of the platform.	This clause requires a human analyst-delivered managed service and is not a functional specification of a solution. Scoring it within a functional compliance sheet at 10 marks does not permit objective evaluation. We request you to kindly move this clause to the managed services/MSSP or CTI service scope of the RFP with defined service levels (number of analyst hours, hunting frequency, deliverable and reporting format) and a separate commercial line item, so that bidders can price it objectively. If it is retained, kindly define the expected analyst effort and deliverables.	Please refer addendum for revised clause
1440	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 11	The solution/service should generate investigation reports for designated VIPs or other high-risk identities/assets, providing an overview of identified digital exposure and associated risk.	VIP/executive digital exposure investigation is a Digital Risk Protection service deliverable involving collection of personal digital footprint data, and carries data-protection considerations under the DPDP Act for the named individuals. We request you to kindly move this clause to the Cyber Threat Intelligence/DRP service scope. If retained, kindly confirm the number of designated VIPs/high-risk identities, the frequency of such reports and the consent/lawful-basis framework the Bank will provide for processing their personal data, so that bidders can price and lawfully deliver the service.	No Change, Please be guided by the RFP
1441	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 5, S.No. 12 and S.No. 13	S.No. 5 - automated and/or AI-assisted generation of tailored intelligence reports based on customer requirements. S.No. 12 - general and industry-related cyber intelligence reports on threat landscape trends, at least twice a month. S.No. 13 - the solution should be able to commission ad-hoc research reports on demand.	Periodic (twice monthly) industry threat-landscape reports and ad-hoc commissioned research reports are analyst-authored service deliverables, and 'on demand' without a defined ceiling is commercially open-ended. We request you to kindly move these clauses to the Cyber Threat Intelligence service scope with defined deliverables, and kindly confirm (a) the maximum number of ad-hoc research reports that may be commissioned per annum, (b) the expected turnaround time, and (c) whether these are to be priced within the platform subscription or as a separate service line item.	a. Periodic industry threat-landscape reports - At least a month b. Ad-hoc commissioned research reports: The requirement shall shall relate to threats, exposures, vulnerabilities and risk areas relevant to the Bank c. Bidder to ensure that all requite cost is factored and the requirement is complied at not additional to the bank Please refer addendum for revised clause
1442	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 18	The solution should provide comprehensive threat actor attribution including known identities, motivations, historical activity, TTPs, associated infrastructure, and MITRE ATT&CK mapping.	Threat-actor attribution dossiers covering actor identities, motivations and associated infrastructure are CTI/DRP deliverables. Exposure-management platforms provide threat-actor and campaign context mapped to MITRE ATT&CK for the vulnerabilities and exposures identified in the Bank's environment. We request you to kindly move this clause to the Cyber Threat Intelligence service scope, or update it as following - "The solution shall provide threat context for identified exposures, including associated threat actors/campaigns, observed exploitation activity, TTPs and MITRE ATT&CK mapping, where such intelligence is available, and shall support enrichment from bank-approved third-party threat-intelligence sources."	Please refer addendum for revised clause
1443	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 19	The solution should detect compromised credentials for employees and VIPs, exposed payment card information, and aggregate data from known breach databases in real time	Detection of compromised credentials and exposed payment-card data through aggregation of breach and dark-web databases is a Digital Risk Protection capability and requires the provider to collect, store and process the Bank's employees' and customers' personal and card data, with attendant DPDP Act and PCI DSS implications. We request you to kindly move this clause to the Cyber Threat Intelligence/DRP service scope of the RFP. If retained under CTEM, kindly confirm the employee/identity count and card-BIN ranges to be monitored, and the data-processing and retention framework the Bank will mandate for such personal and cardholder data.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1444	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 21	The solution should support threat actor interaction via vendor analysts (e.g., engaging via dark web avatars) to gather additional intelligence	Engagement with threat actors through covert dark-web personas is offered by a very small number of DRP providers, cannot be objectively evidenced or evaluated in a technical compliance sheet, and exposes a regulated bank to legal, reputational and regulatory risk arising from interaction with criminal actors on its behalf. We request you to kindly remove this clause from the CTEM functional specifications, as it is restrictive to a limited set of vendors and is not required to achieve continuous threat exposure management outcomes. If the Bank wishes to retain such capability, we request it be moved to an optional service line item, excluded from the technical scoring.	Please refer addendum for the revised clause Clause Stands deleted
1445	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 23	The solution should support reporting of confirmed malicious or phishing assets to relevant external platforms and authorities, where such reporting is supported and authorized.	Reporting and takedown of malicious/phishing domains and assets with registrars, hosting providers, app stores and authorities is an anti-phishing/brand-protection service, delivered under authorisation letters from the brand owner. We request you to kindly move this clause to the anti-phishing/brand protection service scope. If retained, kindly confirm the expected number of takedown/reporting requests per annum and the applicable turnaround SLA, and confirm that the Bank will provide the requisite authorisation to act on its behalf, so that bidders can price the service.	Please refer addendum for the revised clause
1446	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 20, 22, 45 and 47	S.No. 20 - IoC enrichment allowing submission of IPs, domains and hashes to receive contextual threat intelligence and threat actor attribution; S.No. 22 - scanning and reputation analysis of submitted IP addresses; S.No. 45 - manual IoC management operations; S.No. 47 - cross-platform IoC enforcement across the security stack.	IoC submission, enrichment, lifecycle management and - in particular - enforcement of IoCs across the security stack are functions of a Threat Intelligence Platform (TIP) and SOAR, both of which are in scope of this RFP. Enforcement (pushing blocklists to NGFW, proxy, DNS, EDR and email gateways) is performed by those controls under the Bank's change-management process, not by an exposure-management platform. We request you to kindly move S.No. 45 and S.No. 47 to the TIP/SOAR scope, and update S.No. 20 and S.No. 22 as following - "The solution shall support enrichment of submitted indicators (IP addresses, domains, hashes) with available contextual intelligence and reputation information natively and/or through integration with the Bank's threat-intelligence platform, and shall support publishing of validated indicators to the Bank's security controls through the Bank's SOAR/TIP."	Please refer addendum for the revised clause
1447	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 24	The solution should provide pre-built bidirectional integrations with SIEM, SOAR, ticketing (Manage Engine), and threat intelligence platforms	Availability of a 'pre-built' connector is vendor-specific, whereas equivalent bidirectional integration is routinely achieved through documented REST APIs and webhooks with the same functional outcome. We request you to kindly share the Vendor/Model/Version of the SIEM, SOAR, ManageEngine ticketing product and threat-intelligence platform to be integrated, and update the clause as following - "The solution shall provide bidirectional integration with the Bank's SIEM, SOAR, ticketing (ManageEngine) and threat-intelligence platforms through pre-built connectors, documented REST APIs, webhooks or equivalent mechanisms."	Please refer addendum for the revised clause
1448	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 30 and S.No. 33	S.No. 30 - The solution shall provide automated validation of identified exposures, where technically applicable and authorized by the Bank, using controlled, non-destructive testing or equivalent validation mechanisms to determine whether the identified exposure is genuinely exploitable or materially exposed. S.No. 33 - The solution should validate that a vulnerability is actually exploitable or otherwise materially exposed (active exposure validation).	Active, automated exploitation-based validation of findings is the function of Breach and Attack Simulation (BAS) or automated penetration-testing tooling - which the Bank itself references at S.No. 41 of this section as a separate external source to be integrated. Exposure-management platforms establish material exposure and exploitability through evidence-based validation: authenticated/unauthenticated verification of the finding, reachability and internet-exposure analysis, attack-path analysis, exploit availability and exploitation-in-the-wild intelligence. We request you to kindly update the clauses as following - "The solution shall validate whether an identified exposure is genuinely exploitable or materially exposed using evidence-based validation - including verification of the finding, internet exposure and network reachability analysis, attack-path analysis, exploit availability and observed exploitation intelligence - and shall support ingestion of validation results from the Bank's BAS/penetration-testing tools through supported integration." Kindly also confirm that active exploitation testing against the Bank's production environment is not mandated as a day #1 platform capability.	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1449	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 35	The solution should detect malicious files, reconnaissance activity, automated attack tools, and target lists	Detection of reconnaissance activity, automated attack tooling and 'target lists' naming the Bank requires deception/honeypot sensors, network detection telemetry or dark-web collection, none of which are capabilities of a CTEM/exposure management platform. We request you to kindly remove this clause from the CTEM section (reconnaissance and attack-tool detection being already addressed by the Bank's NDR, WAF, NGFW and SOC/SIEM scope), or move it to the Cyber Threat Intelligence/DRP service scope.	Please refer addendum for revised clause
1450	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 41	The solution should support external vulnerability source integrations such as VA/VM scanners, ASM, XDR, BAS, Dark Web Monitoring, and MDM/UEM	Integration is feasible only where the source product, version and API are known, and Dark Web Monitoring and BAS are separate product categories which the Bank may or may not have licensed. We request you to kindly (a) share the Vendor/Model/Version of each source solution to be integrated (VA/VM, ASM, XDR, BAS, Dark Web Monitoring, MDM/UEM), (b) confirm which of these the Bank already owns and which are expected to be supplied by the bidder, and (c) confirm that non-availability of integration with a product the Bank has not licensed, or which does not expose a supported API, shall not be treated as non-compliance.	No Change, Please be guided by the RFP
1451	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 42 and S.No. 43	S.No. 42 - The solution should use machine learning to evaluate the business impact of each remediation action and prioritize high-priority exposures. S.No. 43 - The ML model should continuously study the environment including asset relationships, topology, and security controls to detect false positives and identify root causes.	These clauses mandate a specific implementation mechanism ('machine learning', 'the ML model') and a specific analytic behaviour rather than the security outcome, which is restrictive to a particular OEM's product design. The Bank has adopted a technology-neutral formulation elsewhere in this very section (S.No. 34 - 'using AI/ML or equivalent analytic'). We request you to kindly update the clauses as following, consistent with S.No. 34 - "The solution shall prioritise exposures using AI/ML or equivalent analytics based on asset criticality and business context, exploitability, exposure, asset relationships/topology and the effect of existing security controls, and shall support identification of false positives and of common root causes to enable efficient remediation."	No Change, Please be guided by the RFP
1452	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 38 read with S.No. 41 and S.No. 48	S.No. 38 - The solution should be deployed agentlessly, without requiring sensors or agents on endpoints, servers, or network appliances. S.No. 41 - external vulnerability source integrations such as VA/VM scanners, ASM, XDR, BAS, Dark Web Monitoring, and MDM/UEM. S.No. 48 - The solution should assess and harden network, endpoint, and operating system security controls.	S.No. 38 mandates a fully agentless and sensor-less deployment, while S.No. 48 requires assessment and hardening of endpoint and operating-system security controls - which requires either a credentialed/authenticated scan, an agent, or ingestion from the agent-based VA/VM, XDR and MDM/UEM platforms referenced in S.No. 41. These clauses partially contradict each other. We request you to kindly confirm that the CTEM platform itself may remain agentless and derive endpoint/OS control assessment through integration with the Bank's VA/VM, XDR and MDM/UEM platforms and credentialed configuration audit performed by those tools, and kindly update S.No. 48 as following - "The solution shall consolidate and report on the configuration/hardening posture of network, endpoint and operating system security controls, natively and/or by ingesting configuration and compliance assessment results from the Bank's VA/VM, XDR, MDM/UEM and related platforms."	Please refer addendum for the revised clause
1453	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 49 and S.No. 50	S.No. 49 - The solution should provide a private exposure map of the organization's attack surface. S.No. 50 - The solution should support custom protections tailored to the organization's environment.	The terms 'private exposure map' and 'custom protections' are vendor-specific product terminology and are not objectively evaluable; 'protections' further implies enforcement, which a CTEM platform does not perform. We request you to kindly update the clauses as following - S.No. 49 - "The solution shall provide a consolidated, access-controlled map/inventory of the organisation's internal and internet-facing attack surface, including assets, relationships, exposures and attack paths." S.No. 50 - "The solution shall support custom policies, custom detection/assessment rules, custom risk scoring and custom tagging tailored to the organisation's environment."	S.No 49.: Please refer addendum for revised clause Clarification: S.No 50: " & M500

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1454	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 51, 59, 60, 62 and 63	S.No. 51 - apply virtual patching/compensating controls/exposure mitigation mechanism to the firewall and other security systems through integration with relevant security controls; S.No. 59 - API-based remediation, notification or workflow integration with relevant security controls; S.No. 60 - automated remediation workflows; S.No. 62 - leverage compensating controls and layered defense strategies; S.No. 63 - collaboration tools and ITSM integration for remediation workflows.	These clauses require the CTEM platform to execute configuration changes directly on the Bank's production security controls (firewall, WAF, IPS, EDR). In a regulated banking environment such changes must pass through the Bank's change-management and maker-checker controls, and the accountable system of record for orchestration is the Bank's SOAR/ITSM, which is separately in scope under this RFP. We request you to kindly update the clauses as following - "The solution shall identify applicable compensating controls, virtual patching and exposure-mitigation options for identified exposures, shall provide the corresponding remediation/mitigation instructions and artefacts, and shall trigger and track remediation through API/webhook-based integration with the Bank's SOAR, ITSM and relevant security controls. Actual enforcement of changes on production security controls shall be performed by the respective control through the Bank's approved change-management process." Kindly confirm that compliance achieved through such SOAR/ITSM-orchestrated remediation shall not be treated as non-compliance.	Please refer addendum for revised clause Clarification: S.No 63: No Change, Please be guided by the RFP.
1455	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 61	The solution should ensure remediation actions do not disrupt business continuity	A security platform can assess and present the potential impact of a recommended remediation, but it cannot guarantee the business-continuity outcome of a change executed on the Bank's production systems, which depends on the Bank's change-management, testing and rollback processes and on the affected application's architecture. As worded, the clause places an unqualified guarantee on the bidder/OEM. We request you to kindly update the clause as following - "The solution shall provide impact assessment and risk context for recommended remediation actions, including affected assets, dependencies, prerequisites and rollback considerations, to enable the Bank to plan and execute remediation without disrupting business continuity through its change-management process."	No Change, Please be guided by the RFP
1456	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 55 and S.No. 56	S.No. 55 - The solution should include IOC investigation, infrastructure mapping, and threat actor identification. S.No. 56 - The visual investigation tool should integrate multiple services including WHO IS and Passive DNS.	A graph-based 'visual investigation tool' bundling WHOIS, Passive DNS and threat-actor identification is a specific feature of certain CTI/DRP investigation products and is not a CTEM platform capability; it is also available to the Bank through its threat-intelligence platform in scope under this RFP. We request you to kindly move these clauses to the Cyber Threat Intelligence/DRP or TIP scope, or update them as following - "The solution shall support investigation of identified exposures and indicators, including mapping of the Bank's internet-facing infrastructure and associated relationships (such as domains, sub-domains, certificates, DNS and WHOIS/registration data for the Bank's own digital footprint), and shall support enrichment and threat-actor context through integration with the Bank's threat-intelligence platform."	No Change, Please be guided by the RFP
1457	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 57, S.No. 58 and S.No. 67	S.No. 57 - Up on demand, the vendor should provide a dedicated Customer Success Manager as a single point of contact for onboarding and ongoing support. S.No. 58 - The vendor to provide 24/7 system support. S.No. 67 - The vendor to provide a mechanism to report security incidents identified through the platform and receive prompt response and guidance from the incident response team.	These are commercial/service clauses rather than functional specifications of the solution, and 'dedicated Customer Success Manager' and access to an 'incident response team' are named-resource and incident-response-retainer commitments that cannot be objectively evaluated in a functional compliance sheet or priced without defined limits. We request you to kindly move these clauses to the services/SLA section of the RFP and confirm - (a) whether the Customer Success Manager is required to be dedicated to the Bank full-time or is an assigned named point of contact, and whether onsite presence is expected; (b) the required support SLA and severity-wise response/resolution matrix for 24/7 support; and (c) for S.No. 67, the number of incident-response engagements per annum, whether remote or onsite, and whether these are to be priced within the subscription or as a separate retainer.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1458	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 65 and S.No. 66	S.No. 65 - The solution should aim to reduce Mean Time to Remediate (MTTR) and labor costs. S.No. 66 - The solution should maximize ROI from existing security tools by optimizing the security posture.	These clauses express desired business outcomes rather than verifiable functional specifications, and each carries 10 marks in a scored technical compliance sheet. Compliance cannot be objectively demonstrated or evaluated, and every bidder will necessarily mark itself compliant, which adds no discriminatory value to the Bank's evaluation. We request you to kindly either remove these clauses from the scored functional specifications, or replace them with measurable requirements as following - S.No. 65 - "The solution shall provide MTTR measurement and trending for exposures by severity, asset criticality and business unit, including SLA tracking and ageing analysis." S.No. 66 - "The solution shall provide coverage and control-effectiveness reporting across the Bank's existing security tools, identifying assets not covered by, or gaps in, existing security controls."	Please refer addendum for revised clause
1459	49	7.3.11 Cloud Security (CSPM) Tool		7.3.11 (Preamble) - Integrated cloud security solution providing a centralized and unified single-pane-of-glass view across all cloud assets, workloads, identities, configurations, applications, containers, AI services and cloud-native resources deployed across multi-cloud, hybrid-cloud and on-premises environments.	Unified visibility across cloud assets, workloads, identities, configurations, containers, Kubernetes, AI services and cloud-native resources across multi-cloud and hybrid-cloud is met from a single console. Deviation: 'on-premises environments' - CSPM assesses cloud provider control planes through APIs and has no control plane to assess for traditional on-premises infrastructure. On-premises posture is delivered through configuration/compliance benchmark auditing in the VA & VLM solution, and on-premises Kubernetes through the cloud security platform. Request the Bank confirm that on-premises security posture assessed via CIS/benchmark configuration audit in the VA & VLM solution, consolidated into the same single pane, is acceptable.	No Change, Please be guided by the RFP
1460	50	7.3.11 Cloud Security (CSPM) Tool		7.3.11.2 (10) - Key Deliverable: Incident Response & Automated Playbooks.	The platform provides prioritized findings, remediation guidance, auto-generated remediation code (IaC/CLI), and event/webhook/API triggers that drive downstream automation. Deviation: incident response playbook authoring and execution is SOAR functionality, and SOAR is separately in scope under this RFP. The CSPM tool cannot itself be the playbook execution engine. Request the Bank confirm that this deliverable will be met by publishing CSPM findings and triggers into the Bank's SOAR/ITSM, with the response playbooks built and executed there.	No Change, Please be guided by the RFP
1461	51	7.3.11 Cloud Security (CSPM) Tool		7.3.11.2 (12) - Ensure that the reports are extracted from online / warehouse storage etc. Restore the logs/data from backup for forensic investigation and as per bank requirement without any additional cost.	Findings, assessment history, audit logs and reports are retrievable on demand through the console, scheduled reports and APIs at no additional cost for the retention period applicable to the subscription. Deviation: for an OEM-managed SaaS platform there is no Bank-accessible backup media from which data is 'restored'; data is served from the live platform and its retention tier. Request the Bank (a) specify the mandated retention period, and (b) accept on-demand retrieval/export from the platform as fulfilling this requirement.	Please refer the addendum for revised clause
1462	56	7.4.4 Phishing Simulation	Phishing Simulation	Phishing Simulation	What will be the total numebr of users that will be targeted in Phishing Simualtion & Quarterly Awaraness Trainng	The Bidder shall size and quote the service based on the complete Bank user base. The Bank may conduct campaigns for the required users during the contract period. The Bidder shall ensure that the proposed service is scalable to meet the Bank's requirements.
1463	56	7.4.4 Phishing Simulation	Phishing Simulation	7.4.4 - (K) AI based analysis and correlation of exposed credentials, data leaks and threat indicators.	Regarding AI-based analysis and correlation of exposed credentials, data leaks, and threat indicators — the ThreatCop Phishing Simulation tool captures the password submitted (if any) during a simulation, and smart groups can be created based on employee activity (e.g., link click or data submission). Does the bank require AI-based analysis specifically on these fields captured by the ThreatCop Phishing Simulation tool?	No Change, Please be guided by the RFP
1464	56	7.4.4 Phishing Simulation	Phishing Simulation	7.4.4 - (L) AI based enrichment, correlation and prioritization of threat intelligence	"ThreatCop's TSAT module captures credential submissions (when configured), link-click and attachment-interaction data, and employee-level susceptibility scores (EVS), and allows creation of Smart Groups based on this activity. However, this is simulation-outcome data tracked and segmented within TSAT — not external threat intelligence (e.g., IOC reputation, dark-web exposure, breach-data correlation) enriched or prioritized by AI/ML.	No Change, Please be guided by the RFP
1465	56	7.4.4 Phishing Simulation	Phishing Simulation	7.4.4 - (L) AI based enrichment, correlation and prioritization of threat intelligence	Could the bank confirm: (a) is this requirement intended to apply to simulation-capture data (credentials, clicks, submissions) within TSAT, or (b) does it refer to a separate threat-intelligence capability — e.g., correlating exposed credentials against external data leaks/dark-web sources? This will help us respond accurately to the requirement's actual scope."	No Change, Please be guided by the RFP
1466	Page 147	13.1 Service Level Agreement	Services SLAs:	b.) Site take-down time for identified Phishing URLs – Resolution within 24 hours	We request that the site takedown resolution time for identified phishing URLs be adjusted to a minimum of 48 hours (instead of 24 hours).	No Change, Please be guided by the RFP
1467	Page 147	13.1 Service Level Agreement	Services SLAs:	c.) Site take-down time for Brand Abuse – Resolution within 36 hours	We request that the site takedown resolution time for brand abuse be adjusted to a minimum of 48 hours (instead of 36 hours).	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1468	Page 147	13.1 Service Level Agreement	Penalty		We kindly request that the bank revise the penalty clause to cap penalties per technology at 10% of that specific technology's contract value, rather than the overall contract value. Rationale: Penalising based on the total contract value for an issue with a single technology creates a penalty that significantly exceeds the annual value of that technology, which would be unfair to the primary bidders.	No Change, Please be guided by the RFP RFP Clause 13.2 - For the purpose of this RFP, the total penalties as per LD & SLA will be subject to a maximum of 10% of the overall contract value
1469	95	APPENDIX 1A - Functional (28.5)	APPENDIX 1A - Functional	Web Logs	Dark Web Monitoring solutions are designed to scan external sources on dark web rather than parse private network traffic or server logs.	Please refer addendum for revised clause.
1470	95	28.8	APPENDIX 1A - Functional	Payment Intelligence	Need More Context	No Change, Please be guided by the RFP
1471	98	Section-9	PROJECT TIMELINES	Overall Implementation period shall be 5 Months (Start Date is T0) for all solution & services The bidder shall submit a comprehensive Project Plan, within 7 days of T0 covering each proposed product/solution & Services, detailing all project phases, milestones, tasks, sub-tasks, activities, timelines, dependencies.	We request the Authority to kindly consider extending the overall implementation period from 5 months to 6.5 months, to ensure adequate time for planning, implementation, integration, testing, and successful go-live of all proposed solutions and services.	No Change, Please be guided by the RFP
1472	15	5	PROJECT OBJECTIVE	The bidder shall quote prices strictly in accordance with Appendix 2: Commercial Bill of Material (BoM). The Bank may, if required, procure software, hardware, and/or services in line with the terms and conditions defined in this RFP, based on the unit rates quoted in the BoM. The quoted prices shall remain valid for all orders placed during the entire contract period and shall be binding upon the selected bidder.	Due to the ongoing volatility in the pricing of memory components (DRAM/RAM) and SSD/NAND, the IT infrastructure market, particularly for servers, storage systems, and AI/data-center infrastructure, is experiencing significant price fluctuations. In view of the prevailing market conditions, OEMs are currently unable to commit to price validity beyond a few weeks. We therefore request you to kindly consider discussing the matter with the respective OEMs and explore the possibility of securing the maximum possible price validity for the proposed solution. This would help the bidder mitigate the financial risk and commercial exposure arising from unforeseen fluctuations in memory and SSD prices, which are external factors beyond the bidder's reasonable control. We would appreciate your kind consideration and support in this regard	No Change, Please be guided by the RFP
1473	26	Scope of Work	Note: Point 1	The implementation of each proposed solution, including design, installation, configuration, integration, migration, testing, commissioning, user acceptance testing (UAT), and Go-Live, shall be performed by the respective OEM. The Bidder shall arrange OEM resources, coordinate implementation activities, and ensure timely completion of the project.	We understand OEM PS is mandatory for Security Solution/Services defined in the RFP and bidder own technical resources can deploy the underlying IT infrastructure required for Security Solution deployment. We kindly request you to confirm our understanding or provide the necessary clarification on the OEM PS scope for underlying IT infra.	OEM personnel/professional services shall be mandatory for implementation of the proposed Security Solution/Services. Deployment and configuration of the underlying IT infrastructure, such as servers, storage and SAN switches, may be carried out by the Bidder's/OEM's qualified technical resources, as applicable.
1474	29	Solution & Services Deployment Model and Their HA Requirement	7.2.1 Solutions – Master Deployment Matrix	HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR.	We request bank to kindly amend the requirement as "HA using N+1, Active-Active/Active-Passive at DC and HA using N+1, Active-Active/Active-Passive at DR". The above amendment will ensure optimal utilization of the infrastructure required for solution deployment, provide high availability (HA) for the solution workload, and reduce the overall infrastructure and licensing costs.	Please refer addendum for the revised deployment architecture
1475	31	Solution & Services Deployment Model and Their HA Requirement	7.2.1 Solutions – Master Deployment Matrix	Where N+N Active-Active HA is mandated, all applicable critical Bank-deployed components shall comply with the prescribed HA architecture at DC and DR.	We request bank to kindly amend the requirement as "Where N+1 using Active-Active/Active-Passive HA is mandated, all applicable critical Bank-deployed components shall comply with the prescribed HA architecture at DC and DR.". The above amendment will ensure optimal utilization of the infrastructure required for solution deployment, provide high availability (HA) for the solution workload, and reduce the overall infrastructure and licensing costs.	Please refer addendum for revised clause.
1476	34	7.2.4	Deployment Architecture	Deployment Architecture	Kindly share high resolution image for our understanding	No Change, Please be guided by the RFP
1477	34	7.2.4	Deployment Architecture	Where N+N Active-Active High Availability (HA) is mandated, all applicable Bank-hosted components shall be deployed redundantly within the Primary DC & DR to eliminate single points of failure and ensure seamless failover without material degradation of security monitoring, detection, enforcement or integration capabilities.	We request the Bank to allow bidders to design the solution resiliency architecture based on the required solution uptime and associated SLAs. Mandating an N+N Active-Active High Availability (HA) architecture may significantly increase the underlying IT infrastructure sizing and associated costs. Allowing bidders to propose an appropriate resiliency architecture that meets the defined uptime and SLA requirements will enable optimal infrastructure utilization while ensuring the required availability and cost efficiency.	No Change, Please be guided by the RFP
1478	36	7.2.4.2	Connectivity and Data Flow	The collected telemetry and security data shall be securely transmitted to the applicable Cloud/SaaS security platforms through controlled connectivity mechanisms, including Firewall/NGFW, Secure Internet Gateway, Private/Direct Connectivity, VPN/IPSec and TLS 1.2+ encrypted communication, as applicable.	Kindly confirm whether these components (Firewall/NGFW, Secure Internet Gateway, Private/Direct Connectivity, VPN/IPSec and TLS 1.2+ encrypted communication) are to be provisioned and managed by the bidder as part of the proposed solution, or whether the same will be provided by the Bank as part of its existing network and security infrastructure?	The Bidder shall ensure that the proposed solution is compatible with and can securely integrate with the Bank's network and IT security infrastructure. Any proposed solution-specific configuration required for connectivity shall be carried out by the respective proposed solution OEM as part of implementation.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1479	39	7.2.4.3	On premises deployment of solutions	Restoration - The solution shall support restoration and retrieval of applicable logs, security data, databases, metadata, configurations and other relevant information from the Bank's backup and archival infrastructure. Restoration shall be completed within the RTO specified in this RFP and shall not require additional software or license charges. The Bidder shall perform restoration testing for each proposed solution on quarterly basis.	Based on the clause, we understand that the bidder is required to provision additional storage capacity on the Primary Storage infrastructure for data restoration, equivalent to the data generated during the previous quarter, for each proposed solution. We request the Bank to kindly confirm whether our understanding is correct. The above clarification will help bidders accurately determine the infrastructure sizing, scope, and associated commercial implications.	Please refer Annexure 21, clause 15.21.4 under Retention Requirement, The proposed Primary, backup Storage and Long-Term Storage (LTS) shall be adequately sized not only to meet the prescribed backup and retention requirements but also to support data restoration, retrieval, search, and forensic investigation activities. The bidder shall ensure that all backed up and archived data, logs, configurations, reports, videos, and other artefacts remain recoverable, readable, and accessible throughout the applicable retention period without impacting operational or regulatory requirements.
1480	66	7.6.7	Training- Activities are to be performed by Respective solution OEM (supported by bidder)	The bidder and respective OEMs shall provide comprehensive product training, knowledge transfer, and certification programs for the Bank's IT and Information Security personnel at no additional cost. All technical and product-specific training shall be delivered by OEM.	Kindly confirm whether training from the respective OEMs of the underlying infrastructure is also required as part of the scope. If applicable, we request the Bank to kindly specify the training scope, number of participants, duration, and certification requirements, if any, for each underlying infrastructure component.	Please refer addendum for revised clause
1481	72	7.1.1	Warranty, ATS and AMC. Point 3	Warranty, AMC, and ATS services shall include OEM support, preventive and corrective maintenance, replacement of defective hardware, software updates, upgrades, patches, bug fixes, security updates, technical assistance, subscriptions, and all activities necessary to ensure secure, continuous, and compliant operation of the solution in accordance with the RFP and applicable Bank policies.	Kindly confirm whether Operating System (OS) and Database upgrades are also required to be considered within the scope of work. The above clarification will help bidders to accurately determine the associated commercial implications.	OS and Database upgrades, wherever required for the secure, continuous and compliant operation of the proposed solution, is within the scope of the Bidder/OEM.
1482	83	7.14	DR Drills	The bidder is responsible for conducting the DR Drill on a regular basis and as per the frequency decided by the bank in the presence of bank officials. Coordination with the application team, OEMs and bank's team, is the responsibility of the bidder to ensure the successful execution of the DR drill.	We strongly recommend that the Bank kindly specify the required frequency of Disaster Recovery (DR) Drills as part of the RFP requirements. Defining the DR Drill frequency will provide clarity and ensure that all bidders consider consistent requirements, resource efforts, operational activities, and associated costs while estimating the overall scope of work.	DR drill of the Security shall be on quarterly interval or as and when required by the Bank." The periodic DR drill plan is to be submitted in advance for Bank scheduling/approval.
1483	98	Section 9	PROJECT TIMELINES	Overall Implementation period shall be 5 Months (Start Date is T0) for all solution & services	Due to the prevailing global supply chain constraints and extended OEM lead times, the delivery of certain products may require an additional 16–18 weeks. Accordingly, we request the Bank to consider the implementation timeline starting from the date of actual product delivery, thereby providing adequate time for installation, configuration, integration, testing, and commissioning of the proposed solution. We kindly request the Bank to consider and approve the project timeline as 9 months from T0.	No Change, Please be guided by the RFP
1484	91	7.18.1 IT Infrastructure	5. Compute Infrastructure	Ensure servers include sufficient CPU cores, RAM, and network interface cards (NICs) to handle expected transaction volumes, data processing needs, parallel operation of Backup & Restoration (with Ransomware Protection) and Replication.	We request the Bank to kindly provide clarity on the network zones/VLANs that need to be connected to the proposed servers, including the required number of network interfaces, wherever applicable. This information will enable all bidders to provision the appropriate number and type of NICs/network ports and ensure that the proposed servers are adequately configured and ready for integration with the Bank's existing network architecture. Kindly provide the required network connectivity details to enable accurate sizing, configuration, and commercial estimation by all bidders.	The proposed servers shall be provisioned with sufficient CPU cores, RAM and NICs/network interfaces to meet the performance, transaction volume, data processing, Backup & Restoration (with Ransomware Protection) and Replication requirements specified in the RFP. The required network zones/VLAN connectivity and interfaces shall be shared, on requirement basis, during the detailed design and implementation phase.
1485	261-262	16.21.3 Deployment & Data Retention	Retention Requirement: Monthly Full Backup (Post Retention Period) Note: The proposed Backup and Retrieval Solution shall be sized to support the above retention policy. Upon completion of the two (2) month retention period on Backup Storage, Monthly Full Backups shall be migrated to Long-Term Storage (LTS) and retained in immutable Write Once Read Many (WORM) format for the entire contract period.		We request the Bank to kindly confirm whether a unique full backup file for each month is required to be retained on the Long-Term Storage. If yes, kindly confirm whether the Long-Term Storage should therefore be sized to accommodate 60 unique monthly full backup files, corresponding to the specified 60-month retention period. Further, we request the Bank to kindly confirm whether Synthetic Full Backup is acceptable for the Long-Term Storage requirement, as it can help optimize the storage footprint while maintaining the required backup and retention objectives. This clarification will enable all bidders to accurately size the Long-Term Storage capacity and propose an appropriate backup architecture.	Long Term storage is to be sized to store the backups for the duration of the contract. No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1486	1 - Technical Compliances	Primary Storage	5	Proposed storage solution should be offered with minimum 2 controllers with minimum 256 GB DRAM Cache memory on the entire storage Solution. The solution should scale to at least 512GB Cache memory by adding additional controller.	Kindly Change the Clause to: Proposed storage solution should be offered with minimum 2 controllers with minimum 128 GB DRAM Cache memory on the entire storage Solution. The solution should scale to at least 256GB Cache memory by adding additional controller. Explanation: Cache ask should be Reduced as cache of 64GB or less per controller (128GB total) is enough as the latest CPUs, high-speed memory, and Gen 5 PCIe cards deliver the required performance efficiently. Modern storage controllers optimize cache usage, and industry benchmarks confirm that asked performance can be achieved with lower memory. This reduction not only meets technical needs but also decreases hardware, power, and cooling costs, resulting in a lower TCO for the solution	No Change, Please be guided by the RFP
1487	2 - Technical Compliances	Backup Solution	16	The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data over a secure, API-based disk-to- disk (D2D) connection.	Kindly Change the Clause to: The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data using standard Data protocols such as FC, ISCI, NFS, S3 Explanation: This specific ask qualifies only specific backup appliance not any target storage as enterprise storage do not support data ingestion using API rather leverage protocols such as FC, ISCI, NFS, S3.	Please refer addendum for revised clause.
1488	3 - Technical Compliances	Backup Solution	25	The Proposed Appliance/Backup Storage must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism	Kindly Change the Clause to:The Proposed Appliance/Backup Solution must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism Explanation: Proposed ask should be from Solution instead of storage as any storage does not offer file-level checksum reporting for backup files. This is typically a function of the backup software (e.g., Commvault, Veeam) that stores backups on storage.	Please refer addendum for revised clause.
1489	4 - Technical Compliances	Long Term Storage	4	Additional Point Request	Kindly Change the Clause to: Long Term Storage should support WORM (Write Once, Read Many) capability to have Data Immutability. Explanation: We recommend implementing WORM (Write Once, Read Many) capability for long-term backup storage to ensure data is protected against accidental deletion and ransomware attacks. Additionally, WORM functionality is required to comply with regulatory guidelines for banking institutions. Since backup storage is expected to provide WORM capability, long-term backup storage should also comply with this requirement to maintain robust data protection.	As per tender pg no. 39, point a, "*No Bank data shall be deleted or made inaccessible before expiry of the applicable retention period (refer annexure 21) and without explicit written authorization from the Bank*" It is bidders responsibility to ensure that they comply with the tender requirement
1490	5 - Technical Compliances	1.Primary Storage 2.Backup Storage 3.Long Term Storage		New Point request	Kindly Change the Clause to: The proposed storage systems (for all 3 storage requirements), should have launch dates within past 3 years Explanations: We recommend qualifying storage systems with a launch date within the past three years. This approach ensures a better return on investment and reliable long-term support for a period of 7 to 10 years, as required by the bank. Some OEMs are currently offering systems that are over six years old and lack a clear roadmap or support commitment, which poses a risk to long-term operational stability and longevity.	Please refer addendum for revised clause.
1491	1 - Technical Compliances	Primary Storage	3	The proposed array should be an unified storage which support both SAN & NAS	The proposed array should be an unified / SAN / NAS storage which support both either SAN & OR NAS OR Both based on the proposed solution	No Change, Please be guided by the RFP
1492	1 - Technical Compliances	Primary Storage	7	The proposed array should support FC, iSCSI, (NFS v4.0 or above)/ (SMB 3.1 or above), NVMe/TCP, NVMe/FC from day one.	The proposed array should support FC, iSCSI / (NFS v4.0 or above) / (SMB 3.1 or above) / NVMe/TCP, NVMe/FC from day one.	No Change, Please be guided by the RFP
1493	1 - Technical Compliances	Primary Storage	8	The proposed array should be configured with at least 8 x 32Gbps & 8 x 10Gbps optical front-end ports & Proposed storage should support 100GbE backend.	The proposed array should be configured with at least 8 x 32Gbps & 8 x 10Gbps optical front-end ports & Proposed storage should support 100GbE backend.	Please refer addendum for revised clause.
1494	1 - Technical Compliances	Backup Solution	38	The proposed solution must support LAN-Free (SAN/FC/iSCSI) transport for image-level VM backups on supported block-storage hypervisor platforms, and must ensure that on all other platforms backup data traverses a dedicated backup network/fabric isolated from production LAN traffic, such that no backup payload transits the production Ethernet infrastructure.	Justification: SAN transport carries its own risk. Direct SAN Access requires production LUNs to be presented to the backup proxy; a misconfigured Windows proxy can initialise/sign a production LUN. Many banks deliberately restrict SAN transport for this reason, which is worth mentioning if the Bank asks why the clause should be softened.	The Clause is not referring to the said RFP
1495	1 - Technical Compliances	Backup Solution	40	Backup storage/Appliance capacity expansion - whether by adding disks, adding an enclosure, or adding scale-out nodes - must be non-disruptive, and no additional storage-side licence shall be required to consume the expanded capacity where the backup software's protected-capacity licence already covers the data being protected.'	Is the backup software required to be licensed strictly on a capacity basis, or is an instance/workload-based licence (per VM, per physical server, per database instance, per NAS TB) also acceptable? Justification: Veeam offers Node based licensing with unlimited capacity. While capacity-based licensing is still prevalent in the industry, we have seen a gradual shift to other licensing models which are more flexible and makes procuring the software more cost effective like Instance or Node based model. By giving option for Node -based licensing your overall TCO would reduce dramatically.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1496	79	7.13	Facilities management Point No 27	For the security of the proposed setup, integrate the complete proposed setup with all the currently deployed tools and those procured from time to time.	Please confirm required third-party API licenses, SDKs, connectors and integration enablers will be made available by the Bank where prerequisites for existing-system integration.	Bidder to right size all the required infrastrcuture to meet the requirement mentioned in the RFP
1497	89	7.18	IT Infrastructure Point No 6	IT Infrastructure proposed should have enough CPUs, memory, storage, NIC, Ports, etc. available to accommodate the predicted sizing, SLAs and other requirements of the bank as required. The appliance/devices/cloud environment proposed must have adequate vertical headroom. Any additional cost required for horizontal scaling would be borne by the Bidder in case of breach/ SLA bottleneck	Please define the required percentage or measurable threshold for vertical capacity headroom instead of leaving the requirement open-ended.	The proposed IT infrastructure shall be adequately sized to meet the Bank's requirements, including applicable SLAs, performance and capacity requirements. The infrastructure shall have sufficient capacity headroom to accommodate anticipated growth and operational requirements.
1498	92	7.18.1	Compute	Proposed hardware should have separate FC/LAN Cards enabling separate subnet creation for backup process, if required.	Please confirm that dedicated FC adapters/interfaces shall be provisioned only where technically required by the proposed architecture and existing Bank infrastructure.	Bidder to right size all the required infrastrcuture to meet the requirement mentioned in the RFP
1499	92	7.18.1	Compute	The bidder is required to factor in the necessary compute resources for analytics, AI/ML modelling, etc., and include these details as part of the Bill of Quantities (BOQ).	Please provide AI/ML use cases, model requirements, concurrency and GPU/accelerator utilization assumptions or GPU model, VRAM, concurrency and performance requirements if GPU-based AI/ML processing is mandatory. OR bidder may size GPU infrastructure based on the proposed OEM architecture?	Bidder to right size all the required infrastrcuture to meet the requirement mentioned in the RFP
1500	92	7.18.2	Storage	Bidder will be responsible for the comprehensive end to end design solution of the Storage across the sites which should include Minimal Data Loss, Replication and any other requirements stated in the RFP that relate to the storage.	Please clarify whether DC-DR storage replication is synchronous or asynchronous and confirm the applicable storage RPO.	Storage replication and RPO: The Bidder shall be responsible for the comprehensive end-to-end storage design in accordance with the RFP requirements, including replication and data protection requirements. The proposed solution shall support the RPO and replication requirements specified in the RFP. The mode of replication (synchronous/asynchronous) shall be proposed by the Bidder based on the solution architecture and shall meet the stipulated RPO and SLA requirements.
1501	93	7.18.3	Backup Infrastructure Point No 3	The bidder should configure, schedule and manage backups of all the data including but not limited to files, folders, images, system state, databases and enterprise applications as per the policy defined by PSB.	Please provide expected daily change rate, number of backup jobs, backup window, concurrent backup streams and restore workload for accurate backup sizing.	The Bank has specified the backup requirements and applicable backup policy in the RFP. The bidder shall assess and size the backup solution and associated infrastructure based on the requirements specified in the RFP, including the required data types, retention, backup and recovery requirements. The bidder shall factor appropriate capacity and performance to meet the Bank's backup and restore requirements.
1502	93	7.18.3	Backup Infrastructure Point No 2	Bidder to factor the required solution and infrastructure to ensure taking and securing backup as per the PSB policy (which will be updated from time to time). The sizing of the Backup solution has to be determined by Bidder in accordance with the storage sizing.	Please confirm whether the backup repository capacity may be sized in accordance with the OEM-validated deduplication and compression methodology while ensuring compliance with the stipulated logical data retention and recovery requirements. Kindly confirm that such OEM-validated sizing methodology shall be considered acceptable for determining the required physical backup capacity.	The bidder shall size the Backup Solution and associated infrastructure in accordance with the storage sizing and requirements specified in the RFP. The bidder may consider the applicable OEM-supported/validated deduplication and compression capabilities while determining the physical capacity requirement, provided that the proposed solution continues to meet all stipulated logical data retention, backup, security and recovery requirements of the Bank.
1503	93	7.18.3	Backup Infrastructure Point No 8	The Bidder shall provide/restore such backup data to the Bank as and when required by the Bank, subject to applicable security controls and access procedures.	Please clarify whether the backup repository shall be sized to support -peak concurrent backup and restore workloads or - whether sizing is required only to meet the specified backup window and associated workload.	The bidder shall ensure that the proposed backup solution and infrastructure are capable of meeting the Bank's specified backup, retention and restore requirements. The sizing shall be determined by the bidder based on the requirements specified in the RFP and the proposed solution architecture, including the applicable backup and restore workload. The bidder shall factor adequate capacity and performance to ensure that the required backup and restore operations can be performed within the applicable requirements of the Bank
1504	93	7.18.4	Networking and Security Equipment Point No 1	Ensure network equipment is compatible with existing infrastructure and configured to optimize security, speed, and reliability.	Please provide existing DC/DR -network topology - switch make/model - available ports - uplink speeds	Details shall be shared with the successful bidder
1505	94	7.19.1	Data Centre Requirements Point No 13	The hosting Space and Power arrangement shall be provided by the Bank at DC and DRC. However, the bidder is required to factor in the requisite racks in order to successfully operationalize the proposed hardware.	Please provide available details at both DC and DR. -rack-space -power, cooling, -PDU Types and Ports	Details shall be shared with the successful bidder

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1506	35	7.2.4.1(a): Deployment Pattern	a. SIEM, SOAR and UEBA: The core platforms shall be deployed in the Cloud/SaaS environment, with the required brokers, collectors, aggregators and/or integration/enforcement components deployed at the Bank's DC and DR in N+N Active-Active configuration. The Cloud/SaaS components shall be deployed with HA in accordance with the applicable SLA,		The clause mandates N+N Active-Active configuration for Bank-hosted SIEM/SOAR/UEBA components (brokers, collectors, aggregators, integration/enforcement components) at both DC and DR. Can the Bank permit Active-Passive/Primary-Standby architecture as an alternative for these Bank-hosted components? Justification: Industry-standard DC-DR architecture is typically Active-Passive/Primary-Standby, which optimizes hardware allocation, licensing and overall resource utilization, since the standby node is not required to actively process load in normal operations. Automated failover from Primary to Standby still meets the Bank's HA, RTO and RPO requirements without the cost and complexity of running both sites in true Active-Active mode. Mandating Active-Active across both sites increases infrastructure and licensing cost without a proportionate improvement in resiliency for these specific components, and may reduce the number of OEMs/bidders able to competitively size a compliant solution.	No Change, Please be guided by the RFP
1507	110 / 192	Sl. No. 19, Section 10.2 Eligibility Evaluation Criteria (Clause 19)		The proposed OEM SIEM Solution with a minimum capacity of 30,000 EPS or 1.2 TB/day shall have been successfully implemented and be under management/maintenance in at least one (1) BFSI in India; and the proposed OEM SIEM Solution with a minimum capacity of 30,000 EPS or 1.2 TB/day shall have been successfully implemented on cloud in one (1) in India.	The clause requires a separate cloud-specific reference of 30,000 EPS/1.2 TB per day in India, in addition to the BFSI reference. Can the Bank allow an on-premises reference of the same capacity to also satisfy this second condition? Justification: The intent of this eligibility clause is to verify that the OEM's SIEM solution has proven capability at 30,000 EPS/1.2 TB per day scale. An on-premises deployment at this capacity demonstrates the same (or greater) engineering maturity, scale-handling and operational readiness as a cloud deployment of equal capacity — the deployment model does not materially change the evidentiary value of the reference for this purpose. Restricting the second reference specifically to a cloud implementation in India narrows the pool of eligible OEMs to those with that precise combination of criteria, which may exclude otherwise well-qualified, high-capacity SIEM OEMs and reduce competitive participation, without a corresponding gain in assurance to the Bank.	Please refer addendum for revised clause.
1508	49-51 / 129 / 131	7.3.11 CSPM (Functional) + 10.3 Items 1 & 4 (Scoring)		Implement an integrated Cloud security solution that provides a centralized and unified single-pane-of-glass view across all cloud assets. deployed across multi-cloud, hybrid-cloud, and on-premises environments. Scoring - Item 4 (p.131): CSPM listed among 10 solutions; "...implemented in Client (BFSI/PSU/PSE/Govt Organization) in India" - Point 1 (1 client) = 2 Marks, Point 2 (>2 clients) = 3 Marks (Max 30 Marks across 10 solutions; CSPM's own maximum contribution = 3 Marks).	CSPM is defined in Section 7.3.11 as a Cloud/SaaS-delivered platform providing unified, single-pane-of-glass visibility across multi-cloud, hybrid-cloud, and on-premises environments, irrespective of client geography. Can the Bank clarify whether global/international CSPM implementation references, in addition to India references, will be accepted for scoring under Items 1 and 4 of Section 10.3? Justification: Per its own functional definition in 7.3.11, CSPM's value lies in unified posture visibility and control delivered centrally from the Cloud/SaaS platform - the location of the reference client does not reflect the platform's actual coverage, detection or remediation capability. Restricting the scoring reference to India-based clients only credits OEMs with an established India footprint, and does not credit equally or more capable CSPM platforms with strong global deployment records but fewer India-specific installations - reducing the evaluation's ability to identify the best available CSPM capability for the Bank. This is further reinforced by the fact that CSPM capability is increasingly measured against open, vendor-neutral standards governed by the Cloud Native Computing Foundation (CNCF) - including Kubernetes itself (a CNCF graduated project) and the Open Policy Agent (OPA), a CNCF graduated policy engine (graduated January 2021, used in production by Goldman	No Change, Please be guided by the RFP
1509	51-52 / 132	7.3.12 CNAPP (Functional) + 10.3 Item 5 (Scoring)		The Bank intends to implement a Cloud-Native Application Protection Platform (CNAPP) to provide centralized visibility, continuous risk assessment, and integrated protection for cloud-native applications throughout their lifecycle across multi-cloud, hybrid-cloud, and on-premises environments. Scoring - Item 5 (p.132): "The proposed OEM solution should have been implemented in verifiable client in India...Credential is to be submitted for each of the following solutions: 1. CNAPP 2. CWPP 3. CTEM" - Point 1 (1 client) = 1 Mark, Point 2 (>2 clients) = 2 Marks (Max 6 Marks across 3 solutions; CNAPP's own maximum contribution = 2 Marks).	CNAPP is defined in Section 7.3.12 as a unified, cloud-delivered platform correlating risk across cloud applications, identities, IaC, APIs, containers, and Kubernetes, irrespective of client location. Can the Bank clarify whether global/international CNAPP implementation references, in addition to an India reference, will be accepted for scoring under Item 5 of Section 10.3? Justification: CNAPP's core value, per 7.3.12, is centralized visibility and prioritized remediation delivered from a single cloud-native platform - not a function of where the reference client is headquartered. Limiting the qualifying reference to India-based clients disadvantages globally-proven CNAPP OEMs that may have fewer India-specific deployments despite demonstrated capability across comparable multi-cloud, container and Kubernetes environments elsewhere, without improving the Bank's assurance of the platform's actual protection capability. This is directly evidenced in the runtime-security domain: Falco, the de facto Kubernetes/container runtime threat-detection engine, was created and open-sourced by Sysdig in 2016 and is now a CNCF Graduated project (graduated February 2024) - the highest maturity level CNCF awards. Falco's maintainers and contributors include engineers from Amazon, Apple, IBM, Red Hat and Cisco, and its public adopters include Shopify, GitLab,	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1510	52-53 / 132	7.3.13 CWPP (Functional) + 10.3 Item 5 (Scoring)		Functional (7.3.13, p.52): "The Bank intends to implement a Cloud Workload Protection Platform (CWPP) to provide comprehensive security for cloud workloads deployed across public cloud, private cloud, hybrid cloud, and on-premises environments" with "centralized visibility, continuous monitoring, vulnerability assessment, runtime protection..." Scoring - Item 5 (p.132): "The proposed OEM solution should have been implemented in verifiable client in India...Credential is to be submitted for each of the following solutions: 1. CNAPP 2. CWPP 3. CTEM" - Point 1 (1 client) = 1 Mark, Point 2 (>2 clients) = 2 Marks (Max 6 Marks across 3 solutions; CWPP's own maximum contribution = 2 Marks).	CWPP is defined in Section 7.3.13 as providing centralized, continuous runtime protection across public, private, hybrid cloud, and on-premises environments through a single management plane. Can the Bank clarify whether global/international CWPP implementation references, in addition to Indian references, will be accepted for scoring under Item 5 of Section 10.3? Justification: CWPP's runtime protection, vulnerability assessment and workload-integrity monitoring capabilities (7.3.13) are delivered identically to workloads regardless of the client's country of operation. Requiring the qualifying reference to be an India-based client does not measure the OEM's actual runtime-protection depth, container/Kubernetes coverage or detection efficacy, and may exclude OEMs with strong global CWPP deployment records but limited India-specific references at this stage.	No Change, Please be guided by the RFP
1511	53-54 / 132	7.3.14 CTEM (Functional) + 10.3 Item 5 (Scoring)		Functional (7.3.14, p.53): "The bank intends to establish a continuous Threat Exposure Management (CTEM)...to provide an integrated, unified 'Risk Dashboard' that operationalizes the 5 stages of the CTEM framework (Scoping, Discovery, Prioritization, Validation, and Mobilization)...a single-pane-of-glass view..." Scoring - Item 5 (p.132): "The proposed OEM solution should have been implemented in verifiable client in India...Credential is to be submitted for each of the following solutions: 1. CNAPP 2. CWPP 3. CTEM" - Point 1 (1 client) = 1 Mark, Point 2 (>2 clients) = 2 Marks (Max 6 Marks across 3 solutions; CTEM's own maximum contribution = 2 Marks).	CTEM is defined in Section 7.3.14 as a unified risk framework correlating vulnerability management and breach-and-attack-simulation data through a single-pane-of-glass view. Can the Bank clarify whether global/international CTEM implementation references, in addition to Indian references, will be accepted for scoring under Item 5 of Section 10.3? Justification: CTEM is one of the newest categories in this RFP, and the framework's value (per 7.3.14) lies in its ability to correlate technical vulnerabilities with simulated attack paths across an enterprise's assets - a capability that is platform-driven, not location-driven. Requiring the sole qualifying reference to be an India-based client is likely to exclude several otherwise-capable global CTEM OEMs purely due to the category's early stage of India market adoption, rather than any deficiency in platform capability.	No Change, Please be guided by the RFP
1512	52	7.3.13 CWPP - Modules, Architecture & Deployment (Preamble)		"The proposed solution should provide centralized visibility, continuous monitoring, vulnerability assessment, runtime protection, threat detection, workload integrity monitoring, malware protection, configuration assessment, and security policy enforcement for virtual machines, containers, Kubernetes clusters, serverless workloads, and cloud-native compute resources throughout their lifecycle. The proposed solution shall include all required licenses, subscriptions, connectors, agents, sensors, modules, APIs, and functionalities necessary to provide complete workload protection without requiring any additional third-party components unless specifically proposed by the Bidder."	The CWPP requirement appears to require the complete set of capabilities to be delivered natively through a single solution without third-party components. Can the Bank clarify whether this requirement may be met through a modular, tightly integrated platform from a single OEM, with all required capabilities delivered under the same OEM, rather than requiring a single indivisible engine? Such an architecture would provide the required unified CWPP outcome while allowing technically equivalent solutions to qualify. Justification: As worded, the clause may require all capabilities to be delivered through a single indivisible product, potentially excluding established CWPP solutions that provide equivalent or broader coverage through a modular, tightly integrated single-OEM platform. The requirement should therefore focus on the required security capabilities and outcomes, rather than the OEM's internal product architecture, to avoid unnecessarily restricting competition.	No Change, Please be guided by the RFP
1513	Appendix 1A Page 40	NDR Functional Compliance Sheet	Clause 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high- availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	The Clause mandates Cloud based SaaS model, while RFP Page 30, Page 35, section 7.2.4.1 clause 'd' asks for on Premesis solution "The NDR shall be deployed On-Premises". We request to modify the clause to include On-Prem solution. Justification: To include solutions which are on-Prem based	Please refer Addendum for revised clause
1514	Appendix 1A Page 40	NDR Functional Compliance Sheet	Clause 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high- availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	The Clause asks for Active-Active HA architecture, we request to include Active-Standby Mode. Justification: Management Console is central console, it cannot be deployed in Active-Active mode, as it is a central component.	Please refer Addendum for revised clause
1515	Appendix 1A Page 41	NDR Functional Compliance Sheet	Clause 18	Solution should have the capabilities to create and run security playbooks for automation and better MTTD/MTTR on the basis of criticality of threat/server	Proposed solution adopts below appraoch for automated MTTD, Solution need investigative workflows and all the alerts need to be validated before building any Active Response Solution is having inbuilt playbooks like Host, Session and Packet analysis. once alert is validated Active Response can be triggered. Hope the approach is acceptable	Please refer addendum for revised clause
1516	Page 66	7.6.7	Training	At a minimum, the following training programs shall be conducted for each proposed solution / OEM appointed officials: Duration per Session and Munimum Number of Sessions	Overall there is a requirement of 15 Sessions and Duration per session is 2 or 3 days. This takes the total training per solution to 40 days. This is very large reqirement of training, we request to make it to 3 days for NDR solution	Please refer addendum for revised clause
1517	Page 63	7.6.6	Testing, clause 3	The bidder shall provision and maintain dedicated Development, Testing, UAT, and Pre-Production environments throughout the contract period.	Is UAT Environment required for NDR solution also, given that NDR is a Passive and out of path solution.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1518	Page 30	7.2.1 Solutions – Master Deployment Matrix	#8. Vulnerability assessment (VA) & vulnerability lifecycle management	Bank Location: Standalone at DC and Standalone at DR. Management Console: Deployed at both DC and DR	As per this RFP Technical Specification of VA & VLM,document #1788963129, #12 "The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and failover capabilities" where the 7.2.1 of suggests standalone deployment at DC, DR and console availablity at both DC and DR. These two partially contradict each other. We request you to kindly confirm if standalone VA & VM in DC and DR are expected to function independently. Maintaining two standalone environments with both consoles accessibility will lead to duplication of vulnerabilities, configuration efforts and it will cost upto 2X in terms of licensing. Though its not clear but we assume that you need one VM in DC and one in DR where primary one shares configuration backup on secondary and secondary can take over when the primary goes down, the primary VM solution should be able to scan both the DCs and vice-versa. If this understanding is correct, kindly update the clause as following - 'The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and active-cold standby failover capabilities where only one active console shall be accessible at a time'.	No Change, Please be guided by the RFP
1519	Page 260	16.21.2 Volumetrics-Solution-wise Requirements	10 Vulnerability Assessment & Management (VA-VM) Minimum Numbers of IPs: 4000	10 Vulnerability Assessment & Management (VA-VM) Minimum Numbers of IPs: 4000	As per the RFP #1788963158, page 257 16.21.1 Current IT assets, P&SB has 2500 servers, 300 DB, 200 Apps, 12000 endpoints/desktops and 7200 routers and switches whereas the VA/VM IP coverage is mention as "Minimum" 4000. We seek your guidance and confirmation on the final count of assets/IPs you need coverage from day #1, given "minimum" count may lead to each bidder proposing seperate numbers and very likely excluding important assets from highly important VA & VM exercise. Without a defined and finite asset count, bidders cannot be compared on a like-for-like basis as the ones concerned about the VA/VM security posture of the infra will propose to cover more IPs/Assets while some may cover bare minimum and appear more competitive. We request you to kindly provide the final IP count required for VA/VM from day #1 considering the licenses are bound to assets and deleting the asset will delete all historic vulnerability and trends data, deleted asset will not cover alerts, ITSM integration and cannot be considered as part of VM exercise. As per the CERT'in recommendations (https://www.cert-in.org.in/PDF/guidelinesgovtentities.pdf) as well as industry best practices, entire ICT infrastructure should be part of the vulnerability management exercise and network device inclusion is absolute must given these are critical assets and in some zones exposed directly to internet.	No Change, Please be guided by the RFP
1520	Page 38	On premises deployment of solutions	Storage Capacity & Sizing	• The Bidder shall provide detailed storage sizing based on expected data/log volumes, peak ingestion rate, retention period, indexing, enrichment, compression, replication, backup, archival and anticipated annual growth. Adequate capacity shall be provisioned for the complete contract period.	As per the RFP #1788963158, storage duration on the primary storage of the solution itself is mention for Cloud/SaaS/Hybrid to be 3 months, same is not clearly specified for VA & VM. Kindly confirm how long should the VA & VM solution retain the asset, vulnerability, logs, activities, historic trend etc. As per CERT-IN it must be 6 months. Kindly confirm if you wish the solution to retain this info on its own primary storage to be for 6 months or less.	Please refer addendum for revised clause
1521	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - VA-VM	VA-VM S.No. 9	Each scanning engine shall support web application security assessment together with traditional infrastructure vulnerability and configuration/compliance assessment. The solution shall identify vulnerabilities, missing patches, insecure configurations, and compliance deviations, and generate comprehensive reports containing risk severity, evidence of findings, affected assets, and remediation recommendations to support security governance, audit, and regulatory compliance.	While its possible to perform this via VA VM solution with additional WAS/DAST license, this will be a duplication of solution given you are already asking for seperate 'Application Security Testing Tool'. Hence, we request you to kindly move the 'Web application security assessment' from VA & VM requirements to DAST as this is a DAST requirement and may unnecessorily require to duplicate the licenses, solution and hardware.	No Change, Please be guided by the RFP
1522	Functional Compliance Sheet pp.48-51 (Appendix 1A)	Appendix 1A - VA-VM	VA-VM S.No. 36-52 and S.No. 61-77; S.No. 87 and S.No. 89	All technical compliances of VA-VM S.No. 36-52 and S.No. 61-77; S.No. 87 and S.No. 89	S.N 61-77 are likely duplicates of S.N 36 to 52 with minor changes. Request you to kindly review and confirm if this is intentional or typo. If not intentional, kindly remove duplicates to have the score calculated accordingly.	No Change, Please be guided by the RFP
1523	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 12	The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and failover capabilities.	VM solution is not an inline and always active solution.VM solutions across the industry do not have failovers similar to inline solutions such as firewalls. Hence, we request you to kindly consider the failover scenario as active - cold standby with documented backup-restore and a controlled switchover in place of automatic console failover. We request you to kindly update the clause as - The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and failover capabilities either automatically or using manual and controlled backup restore.	No Change, Please be guided by the RFP
1524	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 15	The proposed solution shall support integration with SIEM, SOAR, Threat Intelligence Platforms, NAC, and other security platforms through APIs or standard integration mechanisms.	Kindly share details (Vendor/Model/Version) of the SIEM, SOAR, TIP and NAC solution you would want to integrate with for us to identify the availablity of standard or API based integration and accordingly finalize the deployment efforts.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1525	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 16	The proposed solution shall integrate with Privileged Access Management (PAM) solutions for secure credential management during authenticated scans.	Kindly share details (Vendor/Model/Version) of the PAM solution you would want to integrate with for us to identify the availablity of integration and also identify the deployment efforts.	Bank is currently procuring PAM solution through separate RFP.
1526	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 17	The proposed solution shall integrate with IT Service Management (ITSM) and ticketing platforms for automated vulnerability tracking and remediation workflows.	Kindly share details (Vendor/Model/Version) of the ITSM solution you would want to integrate with for us to identify the availablity of standard or API based integration and accordingly finalize the deployment efforts.	ITSM - Manage Engine
1527	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 29	The proposed solution shall support vulnerability assessment and compliance reporting aligned with PCI DSS requirements.	We request you to kindly confirm whether you only require to perform PCI DSS internal scanning and reporting on-premises or you also require the PCI- ASV attestation. If Attestation is required, kindly share the exact asset count for which the attestation is needed and how many attestations are to be submitted within 1 year.	No Change, Please be guided by the RFP
1528	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 42	The solution shall support vulnerability assessment of VMware ESXi, Hyper-V, Nutanix AHV, Kubernetes, OpenShift and container platforms.	We request you to kindly confirm whether you need the OS and platform vulnerability assessment of these container solutions or you need a comprehensive container security solution with the ability to identity vulnerabilities of images, registries and their components. If you need comprehensive container security assessment, we request you to kinly move this required to CNAPP solution as its usually part of cloud security solutions and not VM solution.	No Change, Please be guided by the RFP
1529	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 45	The solution shall integrate with enterprise CMDB, ITSM, SIEM, SOAR, PAM and NAC platforms through secure REST APIs.	Kindly share details (Vendor/Model/Version) of the required solutions you would want to integrate with for us to identify the deployment efforts.	Please refer addendum for the revised clause Details shall be shared with successful bidder
1530	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 47	The solution shall support Multi-Factor Authentication (MFA), LDAP, Active Directory, SAML 2.0 and OpenID Connect authentication.	We request you to kindly remove the OpenID and update the clause as following - The solution shall support Multi-Factor Authentication (MFA via SAML and/or LDAP), LDAP, Active Directory, SAML 2.0.	No Change, Please be guided by the RFP
1531	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 48	The solution shall support secure encrypted communication using TLS 1.3 and cryptographic modules compliant with FIPS 140-3 or equivalent internationally recognized standards.	We request you to kindly allow the FIPS 140-2 or equivilent solution transitioning to FIPS 140-3 to participate and update the clause as following - The solution shall support secure encrypted communication using TLS 1.3 and cryptographic modules compliant with FIPS 140-2 or FIPS 140-3 or equivalent internationally recognized standards.	Please refer addendum for revised clause
1532	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 51	The solution shall identify internet-facing assets and continuously monitor externally exposed services.	We request you to kindly remove this clause as its an ASM(Attack Surface Management) requirements which is already asked separate service based solution of the RFP.	Please refer the addendum for revised clause
1533	Functional Compliance Sheet p.49 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 56	The solution shall support digitally signed and password-protected reports with configurable retention and archival.	We request you to kindly update the clause as following - The solution shall support password-protected reports with configurable retention and archival.	Please refer addendum for revised clause
1534	Functional Compliance Sheet p.49 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 60	The solution shall provide comprehensive REST APIs and webhook support for automation and integration with enterprise security platforms.	We request you to kindly update the clause as following - The solution shall provide comprehensive REST APIs or webhook support for automation and integration with enterprise security platforms.	Please refer addendum for revised clause
1535	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 87	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	We request you to kindly remove this clause from VM VM and move it to CTEM as this is a CTEM requirement, a solution that can be cloud/SaaS based. Given the data soveraginity and sensitivity of bank's vulnerabilities data, the platform is correctly requested to be on-prem which shall also be able to function without any internet connectivity. Hence, AI powering the on-prem application to achieve all the listed items is not viable. We request you to kindly remove this point and move it to CTEM.	Please refer the addendum for revised clause
1536	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 88	Unified, correlated findings intelligence. Every scanning engine — across web, API, network and host, cloud, containers, mobile, source code, device configuration and identity — reports into a single normalized findings model..	This is a CTEM requirement as VM solution won't perform VA of source code, identity etc. Kindly move this from VA VM to CTEM requirements.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1537	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 89	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	This is a duplicate of S.N. #87, kindly remove it.	Please refer the addendum for revised clause
1538	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 90	Mobile Application Security Testing: The proposed solution shall support static security analysis of Android and iOS mobile application packages, including APK/AAB and IPA formats, and shall provide security assessment mapped to recognized mobile application security standards and methodologies such as OWASP MASVS and MASTG.	This is not part of any VA/VM solution in industry and belongs to application security testing. We request you to kindly move this to 'Application Security Testing Tool'.	No Change, Please be guided by the RFP
1539	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 91	White-Label Reporting and Approval Workflow: The proposed solution shall support customizable/white-label security assessment reports, including organization-specific branding and configurable report content. The solution shall support role-based maker-checker workflow for report generation, review, approval, and controlled release of finalized reports.	We request you to kindly update the clause as following - White-Label Reporting and Approval Workflow: The proposed solution shall support customizable/white-label security assessment reports, including organization-specific branding and configurable report content. The solution shall support role-based access for report generation, review of the finalized reports.	Please refer addendum for the revised clause White-Label Reporting and Approval Workflow: The proposed solution shall support customizable/white-label security assessment reports, including organization-specific branding and configurable report content. The solution shall support role-based or maker-checker workflow for report generation, review, approval of finalized reports.
1540	Page 92	7.18.1 Compute Infrastructure	10. Non-production:	10. Non-production: a) The non-production environments should have the same software and hardware setup as deployed in production environments meeting all RFP requirements.	While this clause suggests the hardware and software setup of non-prod to be same, "16.21 Annexure 21: Sizing/Volumetrics, Data Retention and Current Infrastructure" suggests the VM based solution to have minimum 10% size. Kindly confirm if the 10% requirement of non-production infra is for only licenses whereas the hardware specs are to be identical to prod or both the licenses as well as hardware/software specs to be 10% of the production infra. Also kindly confirm if the non-production is to be setup only at DC or DC as well as DR.	Please refer addendum for the revised clause
1541	Functional Compliance Sheet pp.47-51 (Appendix 1A)	Appendix 1A - VA-VM	TOTAL MARKS row and S.No. 1 to 94	TOTAL MARKS - 850	While the VA-VM section contains 94 scoreable clauses, each carrying Maximum Marks of 10, which totals 940 marks, whereas the TOTAL MARKS row of the section states 850. We request you to kindly publish the corrected total and confirm the marks allocated per clause, so that bidders can compute the Respective Solution Compliance required by the Appendix 1A summary sheet consistently.	Please refer addendum for the revised clause
1542	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 19, 20, 43 and 44 (missing) and TOTAL MARKS row	CNAPP section is numbered from S.No. 1 to S.No. 60; however S.No. 19, 20, 43 and 44 do not appear in the sheet. TOTAL MARKS - 560.	The CNAPP section is numbered up to S.No. 60 but S.No. 19, 20, 43 and 44 are not present, leaving 56 scoreable clauses which, at 10 marks each, reconciles to the stated TOTAL MARKS of 560. We request you to kindly confirm whether these four clauses have been intentionally deleted or have been inadvertently omitted from the published sheet. If clauses exist against these serial numbers, kindly publish them along with the revised TOTAL MARKS; if they have been deleted, kindly re-issue the sheet with continuous numbering so that bidders' compliance responses and score computation remain traceable to the Bank's evaluation sheet.	Please refer addendum for the revised clause
1543	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 19, 20, 43 and 44 (missing) and TOTAL MARKS row	The solution shall support integration with relevant source-code repositories, development tools, build systems, CI/CD platforms and security workflows, either natively or through supported connectors/APIs.	A CNAPP integrates with source-code repositories and CI/CD platforms for Infrastructure-as-Code (IaC), container image and cloud-configuration assessment. It does not act as a source-code security testing tool, which is the function of the separately procured 'Application Security Testing Tool' in this RFP. We request you to kindly update the clause as following - "The solution shall support integration with relevant source-code repositories, development tools, build systems, CI/CD platforms and security workflows, either natively or through supported connectors/APIs, for the purpose of Infrastructure-as-Code, container image and cloud configuration assessment."	No Change, Please be guided by the RFP
1544	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 17 and S.No. 18	S.No. 17 - The solution shall identify security risks and known vulnerabilities associated with third-party, open-source and externally sourced software components and dependencies used by cloud-native applications. S.No. 18 - The solution shall provide visibility into application dependencies and software components and shall identify affected applications where a vulnerable component or dependency is detected.	Identification of third-party/open-source components and application dependencies is a Software Composition Analysis (SCA)/SBOM capability which belongs to the 'Application Security Testing Tool' scope already sought separately in this RFP, and requiring it again under CNAPP will lead to duplication of licences and cost without additional security benefit to the Bank. We request you to kindly either move these clauses to the Application Security Testing Tool requirements, or update them as following - "The solution shall identify known vulnerabilities in third-party and open-source software components and dependencies present within container images, registries and cloud workloads assessed by the platform, and shall identify the affected cloud-native applications/components."	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1545	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 24	The solution shall provide security visibility for cloud-native APIs and application interfaces, including risks related to exposure, authentication, authorization, access control and relevant configurations, where supported.	Discovery and security assessment of application APIs (including authentication/authorization testing of API endpoints) is the function of a dedicated API Security/API posture solution, and is not a native capability of CNAPP platforms. CNAPP platforms provide visibility of cloud-native API gateway and managed API service configurations and their exposure. We request you to kindly update the clause as following - "The solution shall provide security visibility for cloud-provider API gateway/managed API services and application interfaces discovered from the cloud control plane, including risks related to public exposure, authentication/authorization configuration and access control settings, where supported by the respective cloud platform."	No Change, Please be guided by the RFP
1546	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 26	The solution shall provide visibility into application access to sensitive or critical data and identify security risks arising from inappropriate application access, exposure or relationships, where supported.	As worded, this clause can be read as requiring full Data Security Posture Management (DSPM) with data discovery and classification of the Bank's data stores, which is a separately licensable product category and is not part of a baseline CNAPP. We request you to kindly confirm whether DSPM (data discovery and classification) is intended to be in scope of the CNAPP. If it is not intended, we request you to kindly update the clause as following - "The solution shall provide visibility into application and identity access paths to cloud data stores and shall identify security risks arising from public exposure, excessive access or inappropriate relationships to such data stores, where supported by the respective cloud platform." If DSPM is intended, kindly publish the applicable volumetrics (number/size of data stores) so that bidders can size and price the module consistently.	No Change, Please be guided by the RFP
1547	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 27	The solution shall identify vulnerable application components that are reachable, exposed or potentially exploitable within the application's dependency or relationship graph, where such analysis is supported.	Code-level 'reachability' analysis of a vulnerable function within an application's dependency graph is an SCA/ASPM capability delivered by application security testing tools. CNAPP platforms determine exposure and exploitability from cloud context - internet exposure, network path, identity privilege and attack-path relationships. We request you to kindly update the clause as following - "The solution shall identify vulnerable application components that are internet-exposed, network-reachable or potentially exploitable based on cloud exposure, network path, identity privilege and attack-path relationship analysis, where such analysis is supported by the proposed solution."	No Change, Please be guided by the RFP
1548	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 32	The solution shall provide guided, semi-automated and/or automated remediation capabilities for supported application-security findings.	Fully automated remediation executed directly by a security platform on a production banking cloud environment is generally not permitted under change-management controls, and CNAPP platforms deliver remediation as guided steps and auto-generated remediation artefacts (e.g., IaC fix code/pull requests, CLI commands, policy snippets) which are then applied by the Bank/implementation partner through the Bank's change process. We request you to kindly update the clause as following - "The solution shall provide guided remediation and automatically generated remediation artefacts (such as IaC remediation code, pull requests, CLI commands or policy snippets) for supported application-security findings, which may be applied through the Bank's approved change-management process or through integration with the Bank's SOAR/ITSM platform."	No Change, Please be guided by the RFP
1549	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 59	The solution shall support high availability and service continuity appropriate to the proposed deployment architecture and shall provide mechanisms for recovery of relevant configurations, policies and security information.	Where the CNAPP is delivered as OEM-managed SaaS, high availability, redundancy, backup and disaster recovery are provided by the OEM within the platform and are governed by the OEM's published availability SLA; the Bank cannot be provided Bank-operated HA/DR or restore mechanisms for a SaaS platform. We request you to kindly update the clause as following - "For SaaS-delivered solutions, the OEM shall provide high availability, redundancy and disaster recovery within the platform in line with its published availability SLA, and shall provide mechanisms for export/retrieval of relevant configurations, policies and security information. For on-premises components, if any, the solution shall support HA and documented backup-restore."	Please refer the addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1550	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP - Section scope (S.No. 1 to 50, principally S.No. 1, 6, 7, 8 to 41)	The proposed Cloud Workload Protection Platform (CWPP) shall provide centralized capabilities for protecting, monitoring, detecting, investigating and responding to security threats affecting cloud workloads during runtime. (S.No. 1) and the runtime detection, prevention, response, forensics and threat-hunting clauses at S.No. 6 to 41.	The CWPP section as drafted is predominantly a runtime endpoint/server threat prevention, detection and response (EDR/XDR-class) specification - in-guest malware and ransomware prevention, exploit prevention, host IDS/IPS, file integrity monitoring, process and command-line telemetry, containment actions such as process termination, file quarantine and workload isolation, forensic timelines, process trees and threat hunting. These are delivered by an EDR/XDR agent platform, whereas the CNAPP/CWPP category referenced elsewhere in this RFP delivers agentless workload vulnerability, malware, misconfiguration, identity, secrets and exposure assessment with attack-path context. Given the Bank is separately procuring EDR/XDR and SOC/SIEM capabilities under this very RFP, we request you to kindly clarify and confirm any one of the following, so that bidders are not compelled to bid a second endpoint agent on the same servers: 1. That runtime prevention, containment and forensics requirements of the CWPP section may be met through the Bank's in-scope EDR/XDR platform, with the CWPP providing agentless workload exposure assessment, posture and attack-path context integrated with it; or 2. That the CWPP section may be responded to on a multi-OEM/consortium basis with clear identification of the product meeting each clause (consistent with S.No. 50 of this section); or 3. That the runtime prevention/response clauses be moved	No Change, Please be guided by the RFP
1551	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 2 and S.No. 3	S.No. 2 - The solution shall support protection of workloads deployed across physical, virtual, private-cloud, public-cloud and hybrid-cloud environments, as applicable. S.No. 3 - The solution shall support major public-cloud environments including AWS, Microsoft Azure and Google Cloud Platform, as applicable.	CWPP licensing and sizing depend entirely on the workload inventory in scope, and the clause extends coverage to physical and private-cloud workloads in addition to public cloud. We request you to kindly publish, for the CWPP scope, the workload volumetrics for day #1 and for the contract period - number of physical servers, virtual machines, public-cloud instances (per CSP), container hosts/nodes, Kubernetes clusters and serverless functions - along with the CSP accounts/subscriptions/projects in scope. Kindly also confirm which of these environments are mandatory on day #1, since 'as applicable' may lead each bidder to price a different scope and render the commercial bids non-comparable.	No Change, Please be guided by the RFP
1552	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 8, S.No. 21 and S.No. 22	S.No. 8 - The solution shall detect and prevent, where supported, malware, ransomware, trojans, rootkits and other malicious software or activities affecting protected workloads. S.No. 21 - The solution shall provide protection against ransomware and destructive activities, including detection of abnormal file encryption or mass file modification behavior. S.No. 22 - The solution shall provide exploit detection and/or prevention capabilities for supported workload operating systems and applications.	In-guest prevention of malware, ransomware, trojans and rootkits, behavioural detection of mass file-encryption, and memory/exploit prevention require a kernel-level endpoint prevention engine (EDR/EPP) and are not functions of an agentless cloud workload protection platform, which performs malware and vulnerability detection through workload snapshot/disk analysis without in-line blocking. We request you to kindly move these clauses to the EDR/XDR section of the RFP, or update them as following - "The solution shall detect malware, ransomware, trojans, rootkits, malicious files and destructive activity affecting protected workloads through agentless and/or agent-based assessment, and shall support prevention/blocking natively or through integration with the Bank's EDR/XDR platform."	S.No. 8- No Change, Please be guided by the RFP S.No. 21- No Change, Please be guided by the RFP S.No. 22- No Change, Please be guided by the RFP
1553	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 9 to S.No. 14	S.No. 9 to 14 - monitoring of process execution and process behaviour; detection of suspicious process chains and abnormal parent-child relationships; monitoring of command-line execution, scripts and interpreters; detection of Living-off-the-Land techniques; behavioural/heuristic analysis of anomalous activity; and detection of privilege escalation, persistence, lateral movement and credential misuse.	These clauses describe in-guest runtime behavioural telemetry (process, command-line, script and parent-child process monitoring) which is collected by an EDR/XDR sensor and analysed in the SOC/SIEM. A CWPP that assesses workload exposure agentlessly does not generate kernel-level process telemetry. We request you to kindly move these clauses to the EDR/XDR section, or update them as following - "The solution shall provide the specified runtime behavioural detection capabilities natively or through correlation of telemetry from the Bank's EDR/XDR and SIEM platforms, and shall enrich such detections with workload vulnerability, identity, configuration and exposure context." Kindly also confirm that a capability delivered through such integration will not be treated as non-compliant, consistent with the principle already accepted at CNAPP S.No. 53 of this Appendix.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1554	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 15, S.No. 16 and S.No. 17	S.No. 15 - The solution shall monitor relevant network communications involving protected workloads and identify suspicious or unauthorized communication patterns. S.No. 16 - The solution shall identify communication with known or suspected malicious infrastructure, including malicious IP addresses, domains, URLs, command-and-control infrastructure or equivalent threat indicators, where applicable. S.No. 17 - The solution shall provide host/workload-based intrusion detection and/or prevention capabilities for supported operating systems and workloads.	Host-based intrusion detection/prevention and in-line inspection of workload network traffic for command-and-control communication are functions of HIDS/HIPS agents, NDR and NGFW/IPS controls, all of which are separately in scope in this RFP. A CWPP provides network exposure and reachability analysis from cloud configuration (security groups, NACLs, routes, load balancers, public exposure) rather than packet-level inspection. We request you to kindly move these clauses to the EDR/XDR, NDR or NGFW sections as appropriate, or update them as following - "The solution shall identify workload network exposure, reachable paths and unauthorized/high-risk communication paths from cloud network configuration and available flow logs, and shall support identification of communication with known malicious infrastructure natively or through integration with the Bank's EDR/XDR, NDR, NGFW and SIEM platforms."	S.No. 15- No Change, Please be guided by the RFP S.No. 16- No Change, Please be guided by the RFP S.No. 17- No Change, Please be guided by the RFP
1555	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 18 and S.No. 19	S.No. 18 - The solution shall monitor critical files, directories, system objects and configuration elements for unauthorized modification, creation or deletion, where supported. S.No. 19 - The solution shall provide file integrity monitoring for designated critical files, directories and system objects.	File Integrity Monitoring (FIM) requires a resident agent performing real-time file-system event monitoring on the workload and is a standard EDR/host-integrity capability. It is not delivered by an agentless cloud workload protection platform. We request you to kindly move these clauses to the EDR/XDR section, or update them as following - "File integrity monitoring for designated critical files, directories and system objects shall be provided natively or through integration with the Bank's EDR/XDR or host-integrity solution, with the resulting events available for correlation and reporting."	No Change, Please be guided by the RFP
1556	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 20 and S.No. 24	S.No. 20 - The solution shall detect suspicious creation or modification of system accounts, services, scheduled tasks and other persistence mechanisms, where applicable. S.No. 24 - The solution shall support detection and/or prevention of web-shell and other unauthorized application-level persistence mechanisms, where applicable.	Real-time detection of persistence mechanisms and prevention of web-shell execution are runtime endpoint and web application protection (EDR/WAF) functions. A CWPP can identify such artefacts through periodic workload assessment but cannot prevent their execution. We request you to kindly move these clauses to the EDR/XDR and WAF sections respectively, or update them as following - "The solution shall identify unauthorized accounts, services, scheduled tasks, web-shells and other persistence artefacts present on assessed workloads, and shall support real-time detection/prevention natively or through integration with the Bank's EDR/XDR and WAF platforms."	No Change, Please be guided by the RFP
1557	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 23	The solution shall support virtual patching or equivalent compensating protection mechanisms, where applicable, for vulnerabilities for which immediate patching is not feasible.	Virtual patching is enforced by in-line controls - host IPS agents, NGFW/IPS and WAF - all of which are separately procured under this RFP. A workload protection/exposure platform identifies the vulnerability and recommends the compensating control; it does not itself enforce a virtual patch. We request you to kindly remove this clause from the CWPP section as it is already covered by the Bank's NGFW/IPS and WAF requirements, or update it as following - "For vulnerabilities where immediate patching is not feasible, the solution shall identify the exposure, provide risk context and recommend applicable compensating controls, which may be enforced through the Bank's in-line security controls (host IPS, NGFW/IPS, WAF) through supported integration."	No Change, Please be guided by the RFP
1558	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 25, 26, 27 and 28	S.No. 25 - runtime security monitoring and threat detection for containerized workloads; S.No. 26 - runtime protection for Kubernetes workloads including pods, containers and workload processes; S.No. 27 - detection of suspicious behaviour involving containers, pods, workload processes and workload-to-workload communications; S.No. 28 - security monitoring for serverless workloads/functions.	Container and Kubernetes runtime protection requires a privileged runtime sensor (e.g., eBPF/DaemonSet-based) on every node, which materially differs from the container and Kubernetes security posture, image/registry scanning, admission control and Kubernetes misconfiguration and RBAC assessment delivered by a CNAPP/CWPP. We request you to kindly clarify whether the Bank requires (a) container/Kubernetes runtime sensor-based prevention or (b) container and Kubernetes security posture with image, registry, IaC, admission-control and RBAC assessment plus runtime detection through the Bank's EDR/XDR on the worker nodes. We request you to kindly permit option (b) and update the clauses to allow the capability to be delivered through posture assessment, admission control and integration with the Bank's EDR/XDR and SIEM, failing which the clause is restrictive to a small subset of OEMs. Kindly also publish the number of Kubernetes clusters, nodes and serverless functions in scope for sizing.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1559	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 29 and S.No. 30	S.No. 29 - The solution shall support agent-based and/or agentless protection mechanisms, as applicable to different workload types and supported environments. S.No. 30 - Where an agent is required, the solution shall provide mechanisms for secure deployment, centralized management, health monitoring and controlled upgrade of the workload protection agent.	We note and appreciate that S.No. 29 permits agentless mechanisms. However, several other clauses in this section (S.No. 8 to 41) are achievable only through an in-guest agent, which contradicts the option provided in S.No. 29. We request you to kindly confirm that an agentless-first architecture, supplemented where required by the Bank's EDR/XDR agent already deployed on the workloads, will be accepted as compliant against this section, and that S.No. 30 shall apply only where the bidder proposes its own agent. Kindly also confirm that no additional agent is mandated on workloads that already carry the Bank's EDR/XDR agent, in view of performance and change-management impact on production banking workloads.	No Change, Please be guided by the RFP
1560	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 32 and S.No. 33	S.No. 32 - The solution shall support configurable response actions for detected threats, including alerting, blocking, process termination, file quarantine, workload isolation or other equivalent containment actions, as applicable. S.No. 33 - The solution shall provide workload isolation or containment capabilities to limit the impact or spread of a confirmed or suspected compromise, where supported.	Process termination, file quarantine and host/network isolation are kernel-level containment actions performed by an EDR/XDR agent. An agentless workload protection platform performs cloud-control-plane actions (such as snapshotting, tagging, security-group/identity restriction) and orchestrates containment through the Bank's EDR/XDR and SOAR. We request you to kindly move these clauses to the EDR/XDR section, or update them as following - "The solution shall support configurable response actions for detected threats, including alerting, notification, cloud-control-plane containment actions (such as network/identity restriction, snapshot and tagging) natively, and process termination, file quarantine and workload isolation through integration with the Bank's EDR/XDR and SOAR platforms."	S.No. 32 - No Change, Please be guided by the RFP S.No. 33 - No Change, Please be guided by the RFP
1561	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 34, 35, 36 and 37	S.No. 34 - security investigation using process, file, network, user, workload and event-level information; S.No. 35 - historical workload activity and security-event information sufficient for investigation and forensic analysis; S.No. 36 - process-tree or equivalent process-relationship visualization; S.No. 37 - workload-level threat hunting using available security telemetry and configurable search criteria.	Retention of process/file/network event-level telemetry, process-tree reconstruction and telemetry-based threat hunting are EDR/XDR and SIEM functions and require an in-guest sensor. Additionally, these clauses do not specify a retention period, which makes consistent sizing and pricing impossible. We request you to kindly (a) move these clauses to the EDR/XDR and SIEM sections or permit compliance through integration with the Bank's EDR/XDR and SIEM platforms, and (b) if retained under CWPP, publish the mandated telemetry retention period (hot/warm/archive) and the expected daily event volume per workload, so that all bidders size storage and licences on a common basis.	No Change, Please be guided by the RFP
1562	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 38 and S.No. 39	S.No. 38 - The solution shall support identification and searching of Indicators of Compromise (IoCs), including supported hashes, IP addresses, domains, URLs and equivalent indicators. S.No. 39 - The solution shall support integration with external threat-intelligence sources to enhance workload threat detection and investigation.	Retrospective and real-time IoC sweeps across workloads are performed on EDR/XDR telemetry or in the SIEM, where the Bank's threat-intelligence platform feeds are already consolidated under this RFP. We request you to kindly update the clauses as following - "The solution shall support identification and searching of Indicators of Compromise (hashes, IP addresses, domains, URLs and equivalent indicators) against available workload assessment data natively, and across workload runtime telemetry through integration with the Bank's EDR/XDR, SIEM and threat-intelligence platforms. The solution shall support ingestion of external threat-intelligence to enrich and prioritise workload findings."	No Change, Please be guided by the RFP
1563	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 47 and S.No. 48	S.No. 47 - The solution shall support high availability and service continuity appropriate to the proposed deployment architecture and shall provide mechanisms for recovery of relevant configurations and security policies. S.No. 48 - The solution shall provide mechanisms to identify the protection health/status of onboarded workloads, including agent, connector or communication health where applicable.	For OEM-managed SaaS delivery, high availability, redundancy and disaster recovery are provided within the OEM platform under its published availability SLA and cannot be operated or restored by the Bank. We request you to kindly update S.No. 47 as following - "For SaaS-delivered solutions, the OEM shall provide high availability, redundancy and disaster recovery within the platform in line with its published availability SLA and shall provide mechanisms for export/retrieval of relevant configurations and security policies. For on-premises components, if any, the solution shall support HA and documented backup-restore." For S.No. 48, we request confirmation that reporting of connector/cloud-account onboarding and assessment health (and agent health only where an agent is proposed) shall be treated as compliant.	S.No. 47 - Please refer addendum for revised clause Clarification S.No. 48 - Bidder to propose the aproach ensuring the compliance with the sought requirement. Reporting of connector/cloud-account onboarding and assessment health shall also be considered compliant. Agent health reporting shall apply only where an agent is proposed/deployed.
1564	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 49	The solution shall support consumption and correlation of relevant vulnerability, SBOM, CBOM and threat-intelligence information from the Bank's separately procured security solutions through APIs, supported integrations or equivalent mechanisms, where technically supported.	Consumption of Cryptographic Bill of Materials (CBOM) is an emerging requirement with no single established interchange standard, and correlation is only feasible if the source system and format are known. We request you to kindly confirm (a) the source solutions and the exact formats/standards in which SBOM and CBOM will be provided by the Bank (e.g., CycloneDX, SPDX and version), and (b) that where a standard format/API is not made available by the source solution, non-availability of such correlation shall not be treated as non-compliance, consistent with the qualifier 'where technically supported' in the clause.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1565	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM - Section scope (S.No. 1 to 69 and TOTAL MARKS 690)	Continuous Threat Exposure Management (CTEM) - all functional specifications, S.No. 1 to 69, TOTAL MARKS 690.	A significant proportion of the CTEM section (illustratively S.No. 1, 2, 5, 7 to 13, 18 to 23, 35, 55, 56, 57 and 67) specifies Cyber Threat Intelligence (CTI) and Digital Risk Protection (DRP) service deliverables - multilingual dark-web collection and translation, analyst-authored periodic and ad-hoc research reports, VIP investigation reports, threat-actor dossiers and engagement with threat actors, compromised-credential and payment-card monitoring, takedown/reporting to external authorities, named analyst and incident-response services. These are analyst-delivered managed services and are distinct from a Continuous Threat Exposure Management platform, which (per the recognised CTEM framework) delivers scoping, discovery, prioritisation, validation and mobilisation of exposures across the attack surface. As currently drafted, the section can be fully met only by DRP/CTI service providers and is restrictive to exposure-management platform OEMs, even though the Bank has separately (at VA-VM S.No. 87 and 88) contemplated CTEM as the platform that consolidates and prioritises findings across scanning engines. We therefore request you to kindly split this section into (a) 'CTEM / Exposure Management Platform' and (b) 'Cyber Threat Intelligence and Digital Risk Protection Services', with separate functional specifications, separate marks and separate	No Change, Please be guided by the RFP
1566	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 1, S.No. 2 and S.No. 7	S.No. 1 - The solution should collect intelligence from multiple languages and relevant regional sources, with support for multilingual threat intelligence processing and analysis. S.No. 2 - The solution should support translation or interpretation of collected intelligence into English. S.No. 7 - Each intelligence item should include metadata such as date, author, source, and pre-classification of raw data.	Multilingual collection from closed/regional sources, machine translation of collected raw intelligence, and 'author'-level metadata with pre-classification of raw data are characteristics of a dark-web/DRP collection platform and are not features of a CTEM/exposure management platform. We request you to kindly move these clauses to the proposed Cyber Threat Intelligence/DRP service scope. If they are retained under CTEM, we request you to kindly update them as following - "The solution shall provide vulnerability, exploit and exposure intelligence in English, with source, publication date and classification metadata, and shall support ingestion of multilingual/regional intelligence from bank-approved third-party sources through supported integration mechanisms."	Please refer the addendum for revised clause
1567	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 8 and S.No. 53	S.No. 8 - The solution should allow messaging and collaboration within the context of a specific intelligence item. S.No. 53 - Each alert should include a discussion board for eligible users to collaborate within the alert context.	An in-product messaging/discussion board is a vendor-specific user-interface feature, and for a bank, collaboration and audit trails on security findings are better retained in the Bank's ITSM/SOAR system of record rather than in a third-party SaaS console. We request you to kindly update the clauses as following - "The solution shall support collaboration on a specific exposure, alert or intelligence item through comments/annotations, assignment and status tracking within the platform and/or through bidirectional integration with the Bank's ITSM/SOAR/ticketing platform."	No Change, Please be guided by the RFP
1568	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 9	The solution shall provide access to proprietary, internally generated, licensed or equivalent high-quality threat intelligence sources capable of providing actionable intelligence relevant to the Bank's environment.	We request confirmation of the nature of intelligence expected. Exposure-management OEMs provide proprietary research-generated vulnerability, exploit and exposure intelligence (including exploit availability, exploitation-in-the-wild, ransomware association and predictive exploitability), whereas dark-web/actor intelligence is sourced by DRP providers. We request you to kindly update the clause as following - "The solution shall provide access to the OEM's proprietary/internally generated and/or licensed intelligence covering vulnerabilities, exploits, exploitation activity and exposures relevant to the Bank's environment, and shall support ingestion of additional bank-approved third-party intelligence sources."	No Change, Please be guided by the RFP
1569	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 10	Analysts should perform threat hunting activities to find findings outside of the platform.	This clause requires a human analyst-delivered managed service and is not a functional specification of a solution. Scoring it within a functional compliance sheet at 10 marks does not permit objective evaluation. We request you to kindly move this clause to the managed services/MSSP or CTI service scope of the RFP with defined service levels (number of analyst hours, hunting frequency, deliverable and reporting format) and a separate commercial line item, so that bidders can price it objectively. If it is retained, kindly define the expected analyst effort and deliverables.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1570	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 11	The solution/service should generate investigation reports for designated VIPs or other high-risk identities/assets, providing an overview of identified digital exposure and associated risk.	VIP/executive digital exposure investigation is a Digital Risk Protection service deliverable involving collection of personal digital footprint data, and carries data-protection considerations under the DPDP Act for the named individuals. We request you to kindly move this clause to the Cyber Threat Intelligence/DRP service scope. If retained, kindly confirm the number of designated VIPs/high-risk identities, the frequency of such reports and the consent/lawful-basis framework the Bank will provide for processing their personal data, so that bidders can price and lawfully deliver the service.	No Change, Please be guided by the RFP
1571	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 5, S.No. 12 and S.No. 13	S.No. 5 - automated and/or AI-assisted generation of tailored intelligence reports based on customer requirements. S.No. 12 - general and industry-related cyber intelligence reports on threat landscape trends, at least twice a month. S.No. 13 - the solution should be able to commission ad-hoc research reports on demand.	Periodic (twice monthly) industry threat-landscape reports and ad-hoc commissioned research reports are analyst-authored service deliverables, and 'on demand' without a defined ceiling is commercially open-ended. We request you to kindly move these clauses to the Cyber Threat Intelligence service scope with defined deliverables, and kindly confirm (a) the maximum number of ad-hoc research reports that may be commissioned per annum, (b) the expected turnaround time, and (c) whether these are to be priced within the platform subscription or as a separate service line item.	a. Periodic industry threat-landscape reports - At least a month b. Ad-hoc commissioned research reports: The requirement shall shall relate to threats, exposures, vulnerabilities and risk areas relevant to the Bank c. Bidder to ensure that all requite cost is factored and the requirement is complied at not additional to the bank Please refer addendum for revised clause
1572	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 18	The solution should provide comprehensive threat actor attribution including known identities, motivations, historical activity, TTPs, associated infrastructure, and MITRE ATT&CK mapping.	Threat-actor attribution dossiers covering actor identities, motivations and associated infrastructure are CTI/DRP deliverables. Exposure-management platforms provide threat-actor and campaign context mapped to MITRE ATT&CK for the vulnerabilities and exposures identified in the Bank's environment. We request you to kindly move this clause to the Cyber Threat Intelligence service scope, or update it as following - "The solution shall provide threat context for identified exposures, including associated threat actors/campaigns, observed exploitation activity, TTPs and MITRE ATT&CK mapping, where such intelligence is available, and shall support enrichment from bank-approved third-party threat-intelligence sources."	Please refer addendum for revised clause
1573	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 19	The solution should detect compromised credentials for employees and VIPs, exposed payment card information, and aggregate data from known breach databases in real time	Detection of compromised credentials and exposed payment-card data through aggregation of breach and dark-web databases is a Digital Risk Protection capability and requires the provider to collect, store and process the Bank's employees' and customers' personal and card data, with attendant DPDP Act and PCI DSS implications. We request you to kindly move this clause to the Cyber Threat Intelligence/DRP service scope of the RFP. If retained under CTEM, kindly confirm the employee/identity count and card-BIN ranges to be monitored, and the data-processing and retention framework the Bank will mandate for such personal and cardholder data.	Please refer addendum for revised clause
1574	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 21	The solution should support threat actor interaction via vendor analysts (e.g., engaging via dark web avatars) to gather additional intelligence	Engagement with threat actors through covert dark-web personas is offered by a very small number of DRP providers, cannot be objectively evidenced or evaluated in a technical compliance sheet, and exposes a regulated bank to legal, reputational and regulatory risk arising from interaction with criminal actors on its behalf. We request you to kindly remove this clause from the CTEM functional specifications, as it is restrictive to a limited set of vendors and is not required to achieve continuous threat exposure management outcomes. If the Bank wishes to retain such capability, we request it be moved to an optional service line item, excluded from the technical scoring.	Please refer addendum for the revised clause Clause Stands deleted
1575	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 23	The solution should support reporting of confirmed malicious or phishing assets to relevant external platforms and authorities, where such reporting is supported and authorized.	Reporting and takedown of malicious/phishing domains and assets with registrars, hosting providers, app stores and authorities is an anti-phishing/brand-protection service, delivered under authorisation letters from the brand owner. We request you to kindly move this clause to the anti-phishing/brand protection service scope. If retained, kindly confirm the expected number of takedown/reporting requests per annum and the applicable turnaround SLA, and confirm that the Bank will provide the requisite authorisation to act on its behalf, so that bidders can price the service.	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1576	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 20, 22, 45 and 47	S.No. 20 - IoC enrichment allowing submission of IPs, domains and hashes to receive contextual threat intelligence and threat actor attribution; S.No. 22 - scanning and reputation analysis of submitted IP addresses; S.No. 45 - manual IoC management operations; S.No. 47 - cross-platform IoC enforcement across the security stack.	IoC submission, enrichment, lifecycle management and - in particular - enforcement of IoCs across the security stack are functions of a Threat Intelligence Platform (TIP) and SOAR, both of which are in scope of this RFP. Enforcement (pushing blocklists to NGFW, proxy, DNS, EDR and email gateways) is performed by those controls under the Bank's change-management process, not by an exposure-management platform. We request you to kindly move S.No. 45 and S.No. 47 to the TIP/SOAR scope, and update S.No. 20 and S.No. 22 as following - "The solution shall support enrichment of submitted indicators (IP addresses, domains, hashes) with available contextual intelligence and reputation information natively and/or through integration with the Bank's threat-intelligence platform, and shall support publishing of validated indicators to the Bank's security controls through the Bank's SOAR/TIP."	Please refer addendum for the revised clause
1577	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 24	The solution should provide pre-built bidirectional integrations with SIEM, SOAR, ticketing (Manage Engine), and threat intelligence platforms	Availability of a 'pre-built' connector is vendor-specific, whereas equivalent bidirectional integration is routinely achieved through documented REST APIs and webhooks with the same functional outcome. We request you to kindly share the Vendor/Model/Version of the SIEM, SOAR, ManageEngine ticketing product and threat-intelligence platform to be integrated, and update the clause as following - "The solution shall provide bidirectional integration with the Bank's SIEM, SOAR, ticketing (ManageEngine) and threat-intelligence platforms through pre-built connectors, documented REST APIs, webhooks or equivalent mechanisms."	Please refer addendum for the revised clause
1578	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 30 and S.No. 33	S.No. 30 - The solution shall provide automated validation of identified exposures, where technically applicable and authorized by the Bank, using controlled, non-destructive testing or equivalent validation mechanisms to determine whether the identified exposure is genuinely exploitable or materially exposed. S.No. 33 - The solution should validate that a vulnerability is actually exploitable or otherwise materially exposed (active exposure validation).	Active, automated exploitation-based validation of findings is the function of Breach and Attack Simulation (BAS) or automated penetration-testing tooling - which the Bank itself references at S.No. 41 of this section as a separate external source to be integrated. Exposure-management platforms establish material exposure and exploitability through evidence-based validation: authenticated/unauthenticated verification of the finding, reachability and internet-exposure analysis, attack-path analysis, exploit availability and exploitation-in-the-wild intelligence. We request you to kindly update the clauses as following - "The solution shall validate whether an identified exposure is genuinely exploitable or materially exposed using evidence-based validation - including verification of the finding, internet exposure and network reachability analysis, attack-path analysis, exploit availability and observed exploitation intelligence - and shall support ingestion of validation results from the Bank's BAS/penetration-testing tools through supported integration." Kindly also confirm that active exploitation testing against the Bank's production environment is not mandated as a day #1 platform capability.	Please refer addendum for the revised clause
1579	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 35	The solution should detect malicious files, reconnaissance activity, automated attack tools, and target lists	Detection of reconnaissance activity, automated attack tooling and 'target lists' naming the Bank requires deception/honeypot sensors, network detection telemetry or dark-web collection, none of which are capabilities of a CTEM/exposure management platform. We request you to kindly remove this clause from the CTEM section (reconnaissance and attack-tool detection being already addressed by the Bank's NDR, WAF, NGFW and SOC/SIEM scope), or move it to the Cyber Threat Intelligence/DRP service scope.	Please refer addendum for revised clause
1580	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 41	The solution should support external vulnerability source integrations such as VA/VM scanners, ASM, XDR, BAS, Dark Web Monitoring, and MDM/UEM	Integration is feasible only where the source product, version and API are known, and Dark Web Monitoring and BAS are separate product categories which the Bank may or may not have licensed. We request you to kindly (a) share the Vendor/Model/Version of each source solution to be integrated (VA/VM, ASM, XDR, BAS, Dark Web Monitoring, MDM/UEM), (b) confirm which of these the Bank already owns and which are expected to be supplied by the bidder, and (c) confirm that non-availability of integration with a product the Bank has not licensed, or which does not expose a supported API, shall not be treated as non-compliance.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1581	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 42 and S.No. 43	S.No. 42 - The solution should use machine learning to evaluate the business impact of each remediation action and prioritize high-priority exposures. S.No. 43 - The ML model should continuously study the environment including asset relationships, topology, and security controls to detect false positives and identify root causes.	These clauses mandate a specific implementation mechanism ('machine learning', 'the ML model') and a specific analytic behaviour rather than the security outcome, which is restrictive to a particular OEM's product design. The Bank has adopted a technology-neutral formulation elsewhere in this very section (S.No. 34 - 'using AI/ML or equivalent analytic'). We request you to kindly update the clauses as following, consistent with S.No. 34 - "The solution shall prioritise exposures using AI/ML or equivalent analytics based on asset criticality and business context, exploitability, exposure, asset relationships/topology and the effect of existing security controls, and shall support identification of false positives and of common root causes to enable efficient remediation."	No Change, Please be guided by the RFP
1582	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 38 read with S.No. 41 and S.No. 48	S.No. 38 - The solution should be deployed agentlessly, without requiring sensors or agents on endpoints, servers, or network appliances. S.No. 41 - external vulnerability source integrations such as VA/VM scanners, ASM, XDR, BAS, Dark Web Monitoring, and MDM/UEM. S.No. 48 - The solution should assess and harden network, endpoint, and operating system security controls.	S.No. 38 mandates a fully agentless and sensor-less deployment, while S.No. 48 requires assessment and hardening of endpoint and operating-system security controls - which requires either a credentialed/authenticated scan, an agent, or ingestion from the agent-based VA/VM, XDR and MDM/UEM platforms referenced in S.No. 41. These clauses partially contradict each other. We request you to kindly confirm that the CTEM platform itself may remain agentless and derive endpoint/OS control assessment through integration with the Bank's VA/VM, XDR and MDM/UEM platforms and credentialed configuration audit performed by those tools, and kindly update S.No. 48 as following - "The solution shall consolidate and report on the configuration/hardening posture of network, endpoint and operating system security controls, natively and/or by ingesting configuration and compliance assessment results from the Bank's VA/VM, XDR, MDM/UEM and related platforms."	Please refer addendum for the revised clause
1583	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 49 and S.No. 50	S.No. 49 - The solution should provide a private exposure map of the organization's attack surface. S.No. 50 - The solution should support custom protections tailored to the organization's environment.	The terms 'private exposure map' and 'custom protections' are vendor-specific product terminology and are not objectively evaluable; 'protections' further implies enforcement, which a CTEM platform does not perform. We request you to kindly update the clauses as following - S.No. 49 - "The solution shall provide a consolidated, access-controlled map/inventory of the organisation's internal and internet-facing attack surface, including assets, relationships, exposures and attack paths." S.No. 50 - "The solution shall support custom policies, custom detection/assessment rules, custom risk scoring and custom tagging tailored to the organisation's environment."	S.No 49.: Please refer addendum for revised clause Clarification: S.No 50: " & M500
1584	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 51, 59, 60, 62 and 63	S.No. 51 - apply virtual patching/compensating controls/exposure mitigation mechanism to the firewall and other security systems through integration with relevant security controls; S.No. 59 - API-based remediation, notification or workflow integration with relevant security controls; S.No. 60 - automated remediation workflows; S.No. 62 - leverage compensating controls and layered defense strategies; S.No. 63 - collaboration tools and ITSM integration for remediation workflows.	These clauses require the CTEM platform to execute configuration changes directly on the Bank's production security controls (firewall, WAF, IPS, EDR). In a regulated banking environment such changes must pass through the Bank's change-management and maker-checker controls, and the accountable system of record for orchestration is the Bank's SOAR/ITSM, which is separately in scope under this RFP. We request you to kindly update the clauses as following - "The solution shall identify applicable compensating controls, virtual patching and exposure-mitigation options for identified exposures, shall provide the corresponding remediation/mitigation instructions and artefacts, and shall trigger and track remediation through API/webhook-based integration with the Bank's SOAR, ITSM and relevant security controls. Actual enforcement of changes on production security controls shall be performed by the respective control through the Bank's approved change-management process." Kindly confirm that compliance achieved through such SOAR/ITSM-orchestrated remediation shall not be treated as non-compliance.	Please refer addendum for revised clause Clarification: S.No 63: No Change, Please be guided by the RFP.
1585	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 61	The solution should ensure remediation actions do not disrupt business continuity	A security platform can assess and present the potential impact of a recommended remediation, but it cannot guarantee the business-continuity outcome of a change executed on the Bank's production systems, which depends on the Bank's change-management, testing and rollback processes and on the affected application's architecture. As worded, the clause places an unqualified guarantee on the bidder/OEM. We request you to kindly update the clause as following - "The solution shall provide impact assessment and risk context for recommended remediation actions, including affected assets, dependencies, prerequisites and rollback considerations, to enable the Bank to plan and execute remediation without disrupting business continuity through its change-management process."	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1586	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 55 and S.No. 56	S.No. 55 - The solution should include IOC investigation, infrastructure mapping, and threat actor identification. S.No. 56 - The visual investigation tool should integrate multiple services including WHO IS and Passive DNS.	A graph-based 'visual investigation tool' bundling WHOIS, Passive DNS and threat-actor identification is a specific feature of certain CTI/DRP investigation products and is not a CTEM platform capability; it is also available to the Bank through its threat-intelligence platform in scope under this RFP. We request you to kindly move these clauses to the Cyber Threat Intelligence/DRP or TIP scope, or update them as following - "The solution shall support investigation of identified exposures and indicators, including mapping of the Bank's internet-facing infrastructure and associated relationships (such as domains, sub-domains, certificates, DNS and WHOIS/registration data for the Bank's own digital footprint), and shall support enrichment and threat-actor context through integration with the Bank's threat-intelligence platform."	No Change, Please be guided by the RFP
1587	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 57, S.No. 58 and S.No. 67	S.No. 57 - Up on demand, the vendor should provide a dedicated Customer Success Manager as a single point of contact for onboarding and ongoing support. S.No. 58 - The vendor to provide 24/7 system support. S.No. 67 - The vendor to provide a mechanism to report security incidents identified through the platform and receive prompt response and guidance from the incident response team.	These are commercial/service clauses rather than functional specifications of the solution, and 'dedicated Customer Success Manager' and access to an 'incident response team' are named-resource and incident-response-retainer commitments that cannot be objectively evaluated in a functional compliance sheet or priced without defined limits. We request you to kindly move these clauses to the services/SLA section of the RFP and confirm - (a) whether the Customer Success Manager is required to be dedicated to the Bank full-time or is an assigned named point of contact, and whether onsite presence is expected; (b) the required support SLA and severity-wise response/resolution matrix for 24/7 support; and (c) for S.No. 67, the number of incident-response engagements per annum, whether remote or onsite, and whether these are to be priced within the subscription or as a separate retainer.	No Change, Please be guided by the RFP
1588	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 65 and S.No. 66	S.No. 65 - The solution should aim to reduce Mean Time to Remediate (MTTR) and labor costs. S.No. 66 - The solution should maximize ROI from existing security tools by optimizing the security posture.	These clauses express desired business outcomes rather than verifiable functional specifications, and each carries 10 marks in a scored technical compliance sheet. Compliance cannot be objectively demonstrated or evaluated, and every bidder will necessarily mark itself compliant, which adds no discriminatory value to the Bank's evaluation. We request you to kindly either remove these clauses from the scored functional specifications, or replace them with measurable requirements as following - S.No. 65 - "The solution shall provide MTTR measurement and trending for exposures by severity, asset criticality and business unit, including SLA tracking and ageing analysis." S.No. 66 - "The solution shall provide coverage and control-effectiveness reporting across the Bank's existing security tools, identifying assets not covered by, or gaps in, existing security controls."	Please refer addendum for revised clause
1589	Page 49	7.3.11 Cloud Security (CSPM) Tool		7.3.11 (Preamble) - Integrated cloud security solution providing a centralized and unified single-pane-of-glass view across all cloud assets, workloads, identities, configurations, applications, containers, AI services and cloud-native resources deployed across multi-cloud, hybrid-cloud and on-premises environments.	Unified visibility across cloud assets, workloads, identities, configurations, containers, Kubernetes, AI services and cloud-native resources across multi-cloud and hybrid-cloud is met from a single console. Deviation: 'on-premises environments' - CSPM assesses cloud provider control planes through APIs and has no control plane to assess for traditional on-premises infrastructure. On-premises posture is delivered through configuration/compliance benchmark auditing in the VA & VLM solution, and on-premises Kubernetes through the cloud security platform. Request the Bank confirm that on-premises security posture assessed via CIS/benchmark configuration audit in the VA & VLM solution, consolidated into the same single pane, is acceptable.	No Change, Please be guided by the RFP
1590	Page 50	7.3.11 Cloud Security (CSPM) Tool		7.3.11.2 (10) - Key Deliverable: Incident Response & Automated Playbooks.	The platform provides prioritized findings, remediation guidance, auto-generated remediation code (IaC/CLI), and event/webhook/API triggers that drive downstream automation. Deviation: incident response playbook authoring and execution is SOAR functionality, and SOAR is separately in scope under this RFP. The CSPM tool cannot itself be the playbook execution engine. Request the Bank confirm that this deliverable will be met by publishing CSPM findings and triggers into the Bank's SOAR/ITSM, with the response playbooks built and executed there.	No Change, Please be guided by the RFP
1591	Page 51	7.3.11 Cloud Security (CSPM) Tool		7.3.11.2 (12) - Ensure that the reports are extracted from online / warehouse storage etc. Restore the logs/data from backup for forensic investigation and as per bank requirement without any additional cost.	Findings, assessment history, audit logs and reports are retrievable on demand through the console, scheduled reports and APIs at no additional cost for the retention period applicable to the subscription. Deviation: for an OEM-managed SaaS platform there is no Bank-accessible backup media from which data is 'restored'; data is served from the live platform and its retention tier. Request the Bank (a) specify the mandated retention period, and (b) accept on-demand retrieval/export from the platform as fulfilling this requirement.	Please refer the addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1592	Page 52	ITDR	1.7	Detect and respond to active threats with high fidelity (low false positives and false negatives).	Pre-Bid Query / Clarification: The Bank has separately specified a comprehensive deception platform for detection of active attacker activity, reconnaissance and lateral movement. We understand that the intent of this clause within ITDR is therefore to complement those controls with focused monitoring of the Bank's most critical identities. Considering that enhanced user-activity monitoring is most relevant for high-risk personnel such as executives, privileged users and other critical users, we request the Bank to kindly clarify whether this requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should provide high-fidelity detection and response for risky or anomalous user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, to identify activities associated with careless, malicious or compromised users.	No Change, Please be guided by the RFP
1593	Page 52	ITDR	1.8	Provide contextual information—who, what, when and how—to inform all stages of the attack chain.	Pre-Bid Query / Clarification: The Bank has already sought attack-lifecycle visibility under the separate deception requirements. For ITDR, we understand that additional value would be derived from detailed user-centric context for the Bank's most critical identities, enabling investigation of risky activity performed by such users. We request the Bank to kindly clarify whether this requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should provide contextual information—who, what, when, where and how—around risky user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, to support investigation and response.	No Change, Please be guided by the RFP
1594	Page 52	ITDR	1.9	Provide deep insights into both the potential and used privilege escalation and lateral movement steps in an attack.	Pre-Bid Query / Clarification: Privilege escalation and lateral-movement visibility is already substantially addressed under the separately specified deception solution, including attacker lifecycle visibility, MITRE ATT&CK mapping, deceptive attack paths and detection of lateral movement. To avoid duplication while retaining complementary investigation capability for high-risk identities, we request the Bank to kindly clarify whether this requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should provide deep insights into activities performed by up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, covering application usage, file and data movement, endpoint activity and other risky behaviours to support investigation of compromised, malicious or negligent user activity.	No Change, Please be guided by the RFP
1595	Page 52	ITDR	2.9	Detect all types of attack vectors including pre-attack reconnaissance, zero-day attacks, privilege escalation prevention, lateral movement and data theft.	Pre-Bid Query / Clarification: Pre-attack reconnaissance, lateral movement, malware/attack behaviour and attacker lifecycle visibility are already covered under the Bank's separate deception specifications. We understand that the complementary requirement under ITDR should focus on identity/user risk and potential data-loss activity for the Bank's most critical users rather than duplicate the deception control. We request the Bank to kindly clarify whether this requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should detect risky user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, including suspicious application usage, unauthorized access or movement of sensitive information, removable-media activity, web-based transfer, cloud synchronization and other potential data-exfiltration activities.	The Clause is applicable only to idendity related threat vector only. The volumetrics is provided in the RFP and should be complied
1596	Page 52	ITDR	2.10	Detect multiple attacks simultaneously.	Pre-Bid Query / Clarification: We understand the intent is to ensure that the solution is not restricted to investigation of a single event at a time. Since active attacker detection is separately covered by the deception solution, we request that this clause be clarified in terms of concurrent monitoring and investigation of risky activities across the Bank's designated critical-user population: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should be capable of detecting and investigating multiple risky user and data activities simultaneously across up to 100 critical/high-risk users and their monitored endpoints.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1597	Page 52	ITDR	3.2	Provide unified presentation of both source- and target-based telemetry data in a timeline view.	Pre-Bid Query / Clarification: The Bank has separately specified end-to-end attacker visibility and behavioural analysis under the deception solution. For ITDR investigations involving critical identities, a chronological user-activity view would provide complementary evidence of actions performed by the user. We request the Bank to kindly clarify whether the requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should provide a unified chronological timeline of user- and endpoint-based activity telemetry for up to 100 critical/high-risk users identified by the Bank to support investigation of risky or suspicious user activity.	No Change, Please be guided by the RFP
1598	Page 52	ITDR	3.3	Correlate identity-related telemetry from relevant source and target systems to identify and investigate identity compromise, privilege escalation, credential abuse and lateral movement.	Pre-Bid Query / Clarification: Privilege escalation and lateral-movement detection are already addressed through the separately specified deception controls. To provide complementary investigation capability for the Bank's highest-risk identities, we request the Bank to clarify whether this clause may focus on correlation of user, endpoint, application and data activity for the designated critical-user population: Suggested Clarified Wording / Requested Action: The solution shall support correlation of user, endpoint, application and data-activity telemetry for up to 100 critical/high-risk users identified by the Bank to identify and investigate suspicious user behaviour, sensitive-data movement, policy violations and potential data-exfiltration activities.	No Change, Please be guided by the RFP
1599	Page 52	ITDR	3.4	Integrate with compatible endpoint/extended detection solution to capture screen recordings or screenshots during active attacker sessions as advanced forensic evidence.	Pre-Bid Query / Clarification: The Bank has separately specified attacker-session and forensic visibility through the deception platform. Within ITDR, we understand that visual evidence is intended to strengthen investigation of high-risk user activity. We request the Bank to kindly clarify whether the requirement may be read in an outcome-based manner for the designated critical-user population: Suggested Clarified Wording / Requested Action: The Identity Threat Detection Solution should support screenshots, screen capture or equivalent visual evidence of relevant activity for up to 100 critical/high-risk users during suspicious or high-risk user sessions, as part of forensic investigation and evidence collection.	Please refer addendum for revised clause
1600	Page 52	ITDR	3.5	Integrate with compatible network detection solution to support collection of PCAP data for network-level incident visibility.	Pre-Bid Query / Clarification: The requirement for PCAP is network-centric and does not directly relate to identity posture or focused user-activity monitoring. Further, the Bank's separate deception specifications already require high-interaction decoys, recording of attacker activities, traffic/behaviour visibility, forensic investigation and integration with network/security technologies. To avoid duplication of network-level forensic controls across two solution categories, we request the Bank to kindly delete this clause from the ITDR section. Suggested Clarified Wording / Requested Action: Requested action: Delete Clause 3.5 from the ITDR requirements, as equivalent/complementary network and attacker forensic visibility is already sought under the separate Deception requirements.	Please refer addendum for revised clause
1601	Page 52	ITDR	3.6	Push incident data into SIEM/XDR or SOAR technologies via integrations for improved incident management.	Pre-Bid Query / Clarification: We understand that the objective is to ensure relevant ITDR alerts and investigation context are available to the Bank's SOC ecosystem. For the enhanced monitoring of designated critical users, we request the Bank to kindly clarify whether alerts and activity information may be shared through supported integrations or APIs as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should make alerts and relevant incident/activity data for the monitored critical-user population available to SIEM/XDR, SOAR or other supported security platforms through integrations or APIs for improved incident management.	The proposed solution hould be integrated with SIEM/XDR or SOAR technologies for sharing the incident data via supported integrattion or APIs
1602	Page 52	ITDR	3.7	As part of forensic data collection, include detailed attack path information including protocols leveraged during the attack.	Pre-Bid Query / Clarification: Detailed attack-path and attacker-behaviour visibility is already sought under the separate deception specifications, including deceptive attack paths, MITRE ATT&CK mapping and forensic investigation. To avoid overlap while retaining complementary evidence for investigations involving the Bank's critical identities, we request the Bank to kindly clarify whether the requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should, as part of forensic data collection for up to 100 critical/high-risk users, include detailed user-activity information such as applications used, files accessed, data movement, destination channels and other relevant endpoint activity associated with the incident.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1603	Page 52	ITDR	3.8	Collect user and computer information from Active Directory as part of forensic data gathering to enhance context and assess risk exposure.	Pre-Bid Query / Clarification: We understand that directory information is required to enrich investigations with user and computer context. We request the Bank to clarify that enterprise identity context may be maintained for the overall identity population, while detailed endpoint/user-activity telemetry may be applied to the Bank's designated critical-user population: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should use relevant user and computer identity information to enhance forensic context and risk assessment, and should correlate such context with detailed endpoint/user-activity telemetry for up to 100 critical/high-risk users identified by the Bank.	Please refer addendum for revised clause
1604	Page 52	ITDR	3.9	Detect an adversary's attempt to move laterally toward key assets using as many Windows, Mac or Linux hosts as possible without requiring a persistent agent.	Pre-Bid Query / Clarification: The Bank's separate deception specifications expressly require detection of lateral movement, reconnaissance, credential theft and malicious activity using agentless and/or agent-based deception techniques across the enterprise. The present clause therefore duplicates a capability already being procured under the Deception section. To avoid overlapping scope and duplicate controls, we request the Bank to kindly delete this clause from the ITDR section. Suggested Clarified Wording / Requested Action: Requested action: Delete Clause 3.9 from the ITDR requirements, since lateral-movement detection using deception techniques is already explicitly covered under the separate Deception specifications.	Please refer addendum for revised clause
1605	Page 52	ITDR	3.10	Collect AD user/computer information for forensic context and detect at the earliest point post initial compromise as the attacker first attempts lateral movement and privilege escalation.	Pre-Bid Query / Clarification: Early detection of lateral movement and privilege-escalation activity is substantially covered under the Bank's separate deception requirements. To retain a complementary identity/user-risk objective without duplicating the deception scope, we request the Bank to kindly clarify whether this clause may focus on early detection of risky activity among the designated critical-user population: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should use relevant identity context and detect risky user behaviour at the earliest possible point for up to 100 critical/high-risk users, based on monitored endpoint activities and configured detection policies, enabling investigation and response before such activity results in significant data loss or business impact.	Please refer addendum for revised clause
1606	Page 52	ITDR	3.11	Collect AD user/computer data during forensic gathering while ensuring all deception techniques remain hidden from legitimate users.	Pre-Bid Query / Clarification: The requirement to ensure deception techniques remain hidden from legitimate users is inherently a deception-platform capability. The Bank has already included comprehensive deception requirements covering lures, breadcrumbs, fake credentials, deceptive assets, attacker engagement and techniques designed to remain undetected by attackers. We therefore request the Bank to kindly delete this clause from the ITDR section to avoid duplication. Suggested Clarified Wording / Requested Action: Requested action: Delete Clause 3.11 from the ITDR requirements, as deception techniques and their concealment are already covered under the separate Deception specifications.	Please refer addendum for revised clause
1607	Page 86	Anti Phishing	17.1	Solution should detect at the earliest point in the attack, post initial compromise as the attacker is first attempting to move laterally and escalate privilege.	Pre-Bid Query / Clarification: Since this section is focused on Anti-Phishing, we understand that the objective is to identify suspicious activity following a successful phishing or account-compromise event. Network-level lateral movement and deception capabilities may be addressed by other security controls. We request the Bank to clarify whether this clause may instead focus on early post-compromise user activity visibility for the Bank's most critical users. Suggested Clarified Wording / Requested Action: The solution should support early identification and investigation of suspicious user activities associated with potential account compromise following phishing or other email-originated attacks, with enhanced user activity monitoring for up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles.	Please refer to the relevant Addendum for updated specfications
1608	Page 86	Anti Phishing	17.4	Solution must provide robust supply chain and AI/ML-driven contact chain analysis capabilities to identify and defend against socially engineered, impersonated, or BEC attacks.	Pre-Bid Query / Clarification: As compromise of trusted suppliers and partners is an important source of BEC and phishing risk, we request the Bank to clarify whether the existing supply-chain requirement should explicitly include behavioural analysis of supplier/partner communication patterns to identify attacks originating from compromised trusted accounts. Suggested Clarified Wording / Requested Action: Solution must provide robust supply-chain and AI/ML-driven contact-chain and behavioural analysis capabilities to identify and defend against socially engineered, impersonated or BEC attacks, including threats originating from compromised or impersonated supplier/partner accounts.	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1609	Page 86	Anti Phishing	18	Solution must proactively analyze suspicious URLs using dynamic/behavioral analysis to prevent the spread of malware and other threats.	Pre-Bid Query / Clarification: The RFP separately addresses URL analysis and post-delivery remediation. We request clarification whether these requirements are intended to provide continuous protection throughout the email threat lifecycle, including pre-delivery analysis, click-time URL protection and post-delivery detection/remediation. Suggested Clarified Wording / Requested Action: Solution must provide continuous protection across the email threat lifecycle, including pre-delivery threat detection, real-time/click-time inspection of suspicious URLs, and post-delivery detection and automated remediation of threats that are subsequently determined to be malicious.	Please refer to the relevant Addendum for updated specfications
1610	Page 86	Anti Phishing	19.7	Solution must be able to offer a comprehensive portal that allows users to access information and metadata on events/incidents, facilitating network threat forensics for thorough investigation and analysis of potential security breaches or incidents.	Pre-Bid Query / Clarification: To strengthen investigation of phishing-led incidents involving executives and other critical users, we request clarification whether the existing forensic portal requirement may also include contextual user and endpoint activity for a limited population of Bank-identified critical/high-risk users. Suggested Clarified Wording / Requested Action: Solution must offer a comprehensive investigation portal providing information and metadata on events/incidents for forensic analysis. For up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, the portal should additionally provide contextual user and endpoint activity, including relevant application, file and user-action details, to support investigation of potential phishing-led compromise.	Please refer to the relevant Addendum for updated specfications
1611	Page 86	Anti Phishing	19.9	Solution must empower security operations and incident responders to automate the identification, remediation, and sharing of phishing threats, streamlining the process of detecting, addressing, and disseminating information about potential phishing attacks for improved response and mitigation.	Pre-Bid Query / Clarification: To improve SOC investigation efficiency, we request clarification whether the existing phishing identification and remediation requirement should include centralized attack context showing why a message was identified as malicious, the users targeted, associated threat indicators and remediation status. Suggested Clarified Wording / Requested Action: Solution must empower security operations and incident responders to automate identification, investigation, remediation and sharing of phishing threats, and should provide centralized contextual visibility into the users targeted, associated threat indicators, detection rationale, attack characteristics and remediation actions.	Please refer to the relevant Addendum for updated specfications
1612	Page 86	Anti Phishing	19.1	Solution must provide incident responders with real-time analytics and visibility into email-based attacks targeting the organization.	Pre-Bid Query / Clarification: Email-based attacks against executives and privileged users may require additional context after delivery to determine whether a targeted user has subsequently performed suspicious activity. We request the Bank to clarify whether real-time investigation visibility may include relevant user activity context for up to 100 Bank-identified critical/high-risk users. Suggested Clarified Wording / Requested Action: Solution must provide incident responders with real-time analytics and visibility into email-based attacks targeting the organization. For up to 100 Bank-identified critical/high-risk users, the solution should additionally provide contextual visibility into suspicious user activities associated with potential phishing or account compromise, including relevant user, endpoint, application and file activity.	Please refer to the relevant Addendum for updated specfications
1613	Page 86	Anti Phishing	19.23	Solution must have simplicity of evaluation and additional visibility into internal traffic and other communication channels can reduce risk, and baseline user activity to detect suspicious behavior.	Pre-Bid Query / Clarification: The existing clause already seeks baselining of user activity to detect suspicious behaviour. We request the Bank to clarify the intended depth and scope of this capability and whether enhanced monitoring may be applied to a focused population of up to 100 Bank-identified critical/high-risk users, where deeper visibility provides the greatest security value. Suggested Clarified Wording / Requested Action: Solution must provide additional visibility into relevant internal activity and communication channels to reduce risk and baseline user activity to detect suspicious behaviour. Enhanced user and data activity monitoring should be provided for up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, with configurable detection policies for suspicious, anomalous or policy-violating activities.	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1614	Page 86	Anti Phishing	19.7	Solution must provide protection against harassment mail and mitigate the risks associated with emails from unknown senders specifically for executives or VIPs, safeguarding them from potential threats and ensuring their email communication remains secure.	Pre-Bid Query / Clarification: Since this clause already provides enhanced protection for executives/VIPs, we request the Bank to clarify whether such enhanced protection should extend beyond receipt of suspicious email to investigation of risky user and data activities that may occur following phishing or account compromise, for a limited set of the Bank's most critical users. Suggested Clarified Wording / Requested Action: Solution must provide protection against harassment mail and mitigate risks associated with emails from unknown senders specifically for executives or VIPs. For up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, the solution should additionally provide enhanced visibility into risky user and data activities following suspected phishing or account compromise, including relevant file movement, web/upload activity, removable-media activity and other supported data-transfer channels.	Please refer to the relevant Addendum for updated specfications
1615		Cloud	1	OEM shall ensure compliance of the complete proposed solution & platform with RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and all applicable regulations throughout the contract period.	Pre-Bid Query / Clarification: We request the Bank to clarify that the OEM is required to maintain applicable security, privacy and regulatory controls relevant to the services provided and furnish available compliance/assurance documentation, while the overall regulatory compliance obligation of the Bank remains subject to the Bank's deployment, configuration and usage of the service. Suggested Clarified Wording / Requested Action: OEM shall maintain security, privacy and compliance controls applicable to the proposed hosted service and shall provide available independent assurance reports, certifications and relevant compliance documentation to support the Bank's obligations under applicable RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and other applicable regulatory requirements.	Please refer addendum for revised clause
1616		Cloud	2	The Service uptime agreement for the proposed solution on cloud should have monthly uptime commitments and have transparent monthly credit calculations in case of uptime not being met for any services.	Pre-Bid Query / Clarification: We understand that published/contracted OEM hosted-service SLA commitments and corresponding service-credit methodology shall meet this requirement. Kindly confirm. Suggested Clarified Wording / Requested Action: Retain clause, with clarification that the applicable OEM hosted-service SLA and service-credit schedule will govern the commitment.	No Change, Please be guided by the RFP
1617		Cloud	3	Solution provider should provide the design and process for data deletion in the scope of an independent audit and that the operational effectiveness of these controls is tested. The report for the same should be submitted to bank as and when asked by bank.	Pre-Bid Query / Clarification: For a globally operated hosted security service, control effectiveness is generally evidenced through independent assurance reports such as SOC 2 Type II and documented data-retention/deletion controls. We request the Bank to permit such independent assurance documentation instead of requiring a separate bespoke data-deletion audit report. Suggested Clarified Wording / Requested Action: Solution provider shall maintain documented secure data-retention and deletion controls. Compliance may be demonstrated through applicable independent third-party assurance reports/certifications (such as SOC 2 Type II or equivalent) and documented data-retention/deletion policies made available subject to OEM confidentiality requirements.	Please refer addendum for the revised clause
1618		Cloud	4	Independent audit for testing effectiveness of secure data removal, such that data is rendered permanently inaccessible. (Including any backup or distributed online media).	Pre-Bid Query / Clarification: We request the Bank to accept independently audited secure deletion and media-management controls, together with documented retention/deletion periods, rather than requiring a customer-specific audit of all backup and distributed media. Suggested Clarified Wording / Requested Action: The OEM shall maintain secure data deletion, media handling and backup-retention controls designed to render customer data inaccessible in accordance with documented retention schedules. Effectiveness may be evidenced through independent assurance reports such as SOC 2 Type II/ISO 27001 or equivalent and relevant OEM security/privacy documentation.	Please refer addendum for the revised clause
1619		Cloud	5	Bank shall have an option to implement 'Bring Your Own Key' as and when required.	Pre-Bid Query / Clarification: The proposed service protects data at rest and in transit using strong encryption; however, customer-managed infrastructure encryption keys are not a standard capability of the hosted anti phishing service. We request deletion of the BYOK requirement, or acceptance of OEM-managed enterprise-grade encryption and key-management controls. Suggested Clarified Wording / Requested Action: Requested Action: Delete the BYOK requirement. Alternatively: 'Data processed/stored by the hosted service shall be protected using industry-standard encryption in transit and at rest, with secure OEM-managed key-management controls subject to independent security assurance.'	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1620		Cloud	6	Web Application Firewall shall be implemented on the cloud for Web based applications. WAF application signature should be updated and reviewed regularly. The Report shall be submitted to bank on a periodic interval.	Pre-Bid Query / Clarification: Since the proposed platform is an OEM-managed hosted security service, underlying WAF technology, signatures and configurations form part of the OEM's internal security architecture and may not be exposed as customer-specific reports. We request the Bank to accept periodic VAPT/penetration-test assurance or equivalent independent security assessment evidence covering the hosted application instead of WAF signature reports. Suggested Clarified Wording / Requested Action: The hosted web application/platform shall be protected through appropriate application-security controls. The OEM shall conduct periodic vulnerability assessment and penetration testing/security assessments and, subject to confidentiality restrictions, provide an executive summary/attestation or applicable independent assurance evidence to the Bank on request. Customer-specific WAF signature reports shall not be mandatory.	Please refer addendum for revised clause
1621		Cloud	7	The systems in cloud infrastructure should be periodically updated with the latest anti-malware signatures, the bidder shall submit the periodic report on the same with bank.	Pre-Bid Query / Clarification: For an OEM-managed hosted security service, infrastructure anti-malware/endpoint controls are centrally managed and independently audited. We request the Bank to accept OEM security assurance and vulnerability/malware-control attestations rather than periodic host-level signature reports. Suggested Clarified Wording / Requested Action: The OEM shall maintain appropriate malware protection, vulnerability management, patching and security monitoring controls for the hosted infrastructure. Compliance may be evidenced through independent assurance reports/certifications and applicable security-control attestations instead of customer-specific anti-malware signature update reports.	Please refer addendum for revised clause
1622		Cloud	8	Data Loss Governance and risk management framework shall be defined by bidder for workload on the cloud and same shall be shared with bank on periodic basis. Data loss prevention controls should be implemented to secure the data in the cloud environment from unauthorized or inadvertent exfiltration.	Pre-Bid Query / Clarification: We request clarification that the requirement is intended to ensure protection against unauthorized/inadvertent data exfiltration through the proposed service and appropriate security controls for hosted customer data, rather than requiring disclosure of the OEM's internal cloud governance framework. Suggested Clarified Wording / Requested Action: The proposed solution shall provide configurable controls to identify and prevent unauthorized or inadvertent transmission/exfiltration of sensitive information through any channels. The OEM shall maintain appropriate access control, encryption and data-protection controls for customer data processed within the hosted service and provide applicable assurance documentation on request.	Please refer addendum for revised clause
1623		Cloud	9	Log generation, storage and review process should be certified by CERT IN empaneled auditor, report for the same shall be submitted by bidder as and when required by bank.	Pre-Bid Query / Clarification: For global SaaS/POD services, security logging and monitoring controls are typically independently audited under recognized assurance frameworks. We request the Bank to accept SOC 2 Type II/ISO 27001 or equivalent independent assurance in lieu of a mandatory CERT-In-empanelled audit of the OEM's internal log-generation/storage/review process. Suggested Clarified Wording / Requested Action: The OEM shall maintain documented security logging, monitoring, retention and review controls. Effectiveness shall be evidenced through applicable independent third-party assurance reports/certifications such as SOC 2 Type II, ISO 27001 or equivalent. CERT-In-empanelled audit may be required only for bidder-managed components deployed specifically within the Bank environment, where applicable.	Please refer addendum for the revised clause
1624		Cloud	10	IT Act 2000 & its amendments, and other Acts/Regulatory guidelines.	Pre-Bid Query / Clarification: Kindly clarify that the OEM must comply with legal/regulatory requirements applicable to it as the provider of the proposed hosted service and provide reasonable documentation to support the Bank's compliance obligations. Suggested Clarified Wording / Requested Action: OEM shall comply with applicable legal and regulatory obligations relevant to its provision of the proposed service and shall provide available security/privacy/compliance documentation reasonably required to support the Bank's applicable obligations.	Please refer addendum for the revised clause
1625		Cloud	11	CERT IN Empaneled auditor report's is required for the following:	Pre-Bid Query / Clarification: We request the Bank to permit internationally recognized independent assurance reports/certifications for OEM-managed hosted services. CERT-In empanelled audit reports may remain applicable to India-specific bidder-managed/on-premises components where such audit is feasible and required. Suggested Clarified Wording / Requested Action: For OEM-managed hosted/SaaS services, independent assurance reports/certifications such as SOC 2 Type II, ISO 27001 or equivalent shall be accepted. CERT-In empanelled audit reports shall be applicable only to components/services for which such India-specific audit is contractually and technically feasible.	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1626		Cloud	12	The application and DB is/will be hosted separately on a dedicated infrastructure (physical/logical) for PSB. Evidence of dedicated infrastructure (physical/logical) for PSB should be submitted.	Pre-Bid Query / Clarification: The proposed platform is an OEM-managed hosted security service designed with logical access controls and customer data isolation. Requiring dedicated physical application/database infrastructure would restrict standard SaaS/POD architectures without necessarily improving the security outcome. We request acceptance of secure logical tenant/customer isolation supported by independent assurance evidence. Suggested Clarified Wording / Requested Action: The proposed hosted service shall provide secure logical segregation/isolation of Bank data and administrative access from other customers through appropriate access-control and tenant-isolation mechanisms. Dedicated physical application/database infrastructure shall not be mandatory where equivalent logical isolation is implemented and independently assured.	Please refer addendum for revised clause
1627		Cloud	13	Feasibility to audit/review IT controls of the third party or obtaining independent review report for the same from CERT-In empaneled security consultant, to ensure it meets Bank's information security requirement.	Pre-Bid Query / Clarification: We request that the Bank permit review of current independent assurance reports/certifications as the primary mechanism for reviewing OEM IT controls. Any direct audit should remain subject to the OEM's standard contractual audit provisions, confidentiality, security, scope and advance-notice requirements. Suggested Clarified Wording / Requested Action: The Bank may review applicable independent third-party assurance reports/certifications covering the hosted service. Where additional audit is required, such audit shall be subject to mutually agreed scope, confidentiality/security restrictions, reasonable advance notice and the OEM's standard contractual audit provisions. A CERT-In empanelled consultant may review evidence made available under these conditions.	Please refer addendum for revised clause
1628	Page 117	10.2	Eligibility Criteria-Clause-22	The proposed OEM solution should have been implemented in at least one verifiable client in India. Credential is to be submitted for the following solutions: a. CNAPP b. CWPP c. CTEM	CTEM is a new framework and customers are still in evaluation/ Implementation phase. Suggested change Client in India or Global BFSI The proposed OEM solution should have been implemented in verifiable client in India or Global. Credential is to be submitted for each of the following solutions: 1. CNAPP 2. CWPP 3. CTEM	No Change, Please be guided by the RFP
1629	Page 120	10.2	Eligibility Criteria-Clause-23	The proposed OEM services should have been implemented in at least one (1) PSU/ PSE/ Government Organizations / BFSI in India. Credential is to be submitted for the following services: 1. Breach Attack & Simulation 2. Continuous Automated Red Teaming 3. Attack surface management 4. Phishing simulation 5. Anti-phishing services 6. Dark web monitoring 7. Brand protection & monitoring 8. Threat Intelligence feed 9. Threat Hunting services	As the offsite services are specified under the functional compliance requirements and are expected to be provided by the bidder, the corresponding eligibility criteria should be assessed at the bidder level. Suggested Changes: The proposed bidder services (below mentioned to the services) should have been implemented by the bidder in in at least one verifiable client in India.	No Change, Please be guided by the RFP
1630	Page 23	SIEM / Functional Specification	23	Where a native parser or connector is unavailable, the proposed solution shall provide supported mechanisms, SDKs, APIs, templates, or configuration interfaces to develop and maintain custom integrations	For a recuced overall TCO and ensure the timely availability without any delay, please rephrase it to: OEM /OEM authorized partner to provide parsers for data ingestion for all the current data sources and their respective upgrades (in maximum 15 business days from data of intimation of the same) during the contract period. If any new data source is added during the contract period, the OEM will provide parsers for data ingestion in maximum 15 business days from data of intimation of the same, without dependency of the bidder.	No Change, Please be guided by the RFP
1631	Page 28	SIEM / Incident Response	131	The proposed cloud-delivered solution shall provide secure multi-tenant architecture with appropriate logical tenant isolation, encryption in transit and at rest, secure authentication, MFA, granular RBAC, audit logging and protection of Bank security data in accordance with the approved service architecture, security controls and SLA.	Why there is a need for multi-tennacy, this is specially required in a service provider environment needing multiple customers to be managed, please remove or rephrase it to: The proposed solution must provide fine grained role-based access into actions and assets, so users can be granted with investigative actions and not containment actions."	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1632	Page 59	7.6 OEM Responsibilities	1.	All activities relating to solution architecture, design, implementation, configuration, customization, integration, migration, testing, deployment, documentation, training, and Go-Live shall be performed by the respective Solution OEM in coordination with the Bidder	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: 1. All activities relating to solution architecture, design, implementation, configuration, customization, integration, migration, testing, deployment, documentation, training, and Go-Live shall be performed by the respective Solution OEM /OEM authorized partner in coordination with the Bidder. 2. The OEM /OEM authorized partner shall design, implement, and support an enterprise-grade, scalable, resilient, secure, and future-ready solution compatible with the Bank's existing and target IT and Cyber Security architecture across on-premises, cloud, and hybrid environments. 3. The OEM /OEM Authorized partner shall prepare and submit all design documents including HLD, LLD, deployment architecture, integration architecture, configuration guides, SOPs, operational manuals, as-built documentation, and implementation artefacts. 4. The OEM /OEM authorized partner shall provide all native and custom integrations, APIs, connectors, parsers, workflows, playbooks, dashboards, reports, automation, authentication, authorization, RBAC, logging, monitoring, alerting, and interoperability required for successful operation of the solution. 5. The OEM /OEM authorized partner shall perform sizing validation, deployment, migration, configuration, tuning, optimization, health checks, and stabilization to ensure	Please refer addendum for revised clause
1633	Page 60	7.16 OEM Services & Deployment (Architecture Assessment)	87	Assessment & performance review 1. Review of respective solutions configurations (Custom parsers, playbooks, controls, rules and process etc.) of the OEM solution 2. System Optimization review and suggestion including remedial actions. 3. Review the bidder's implementation of suggestions of remedial actions. 4. List of Solution for which Assessment is to be conducted, Year 2 Onwards are	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: OEM /OEM authorized partner for Services & Deployment (Architecture Assessment) Assessment & performance review 1. Review of respective solutions configurations (Custom parsers, playbooks, controls, rules and process etc.) of the OEM solution 2. System Optimization review and suggestion including remedial actions. 3. Review the bidder's implementation of suggestions of remedial actions. 4. List of Solution for which Assessment is to be conducted, Year 2 Onwards are	No Change, Please be guided by the RFP
1634	Page 60	7.6.1 Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder)		Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder) Requirement Analysis - Activities are to be performed by Respective Solution OEM/OEM Authorized Partner (supported by bidder) 1. The respective Solution OEM, assisted by the bidder, shall conduct a detailed assessment of the Bank's business, functional, technical, operational, security, compliance, and integration requirements and design a scalable, resilient, and futureready solution. The proposed solution shall fully comply with the requirements specified in the RFP and support future business and technology needs of the Bank. 2. As part of the requirement gathering phase, the OEM shall conduct workshops, discovery sessions, interviews, and discussions with the Bank's stakeholders and appointed consultants to understand business requirements, existing infrastructure & solutions, integrations, operational processes, and security requirements. 3. The OEM shall review the Bank's existing IT, security, application, network, cloud, and infrastructure landscape and recommend an optimized target-state architecture leveraging both existing and proposed components wherever feasible.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner Requirement Analysis - Activities are to be performed by Respective Solution OEM/OEM Authorized Partner (supported by bidder) 1. The respective Solution OEM /OEM authorized partner, assisted by the bidder, shall conduct a detailed assessment of the Bank's business, functional, technical, operational, security, compliance, and integration requirements and design a scalable, resilient, and futureready solution. The proposed solution shall fully comply with the requirements specified in the RFP and support future business and technology needs of the Bank. 2. As part of the requirement gathering phase, the OEM/OEM authorized partner shall conduct workshops, discovery sessions, interviews, and discussions with the Bank's stakeholders and appointed consultants to understand business requirements, existing infrastructure & solutions, integrations, operational processes, and security requirements. 3. The OEM /OEM authorized partner shall review the Bank's existing IT, security, application, network, cloud, and infrastructure landscape and recommend an optimized target-state architecture leveraging both existing and proposed components wherever feasible. 4. The OEM /OEM authorized parrtner but not be limited to: a. Requirements elicitation and analysis	No Change, Please be guided by the RFP
1635	Page 61	7.6.2 System Design - Activities are to be performed by Respective solution OEM (supported by bidder)	7.6.2	System Design - Activities are to be performed by Respective solution OEM 1. The bidder and respective OEM shall be responsible for the end-to-end design, sizing, customization, configuration, integration, implementation, deployment, maintenance, and support of the proposed solution, including coordination with all associated OEMs, service providers, and stakeholders. 2. All proposed NextGEN SOC solutions shall support seamless interoperability, realtime integration, event sharing, correlation, orchestration, and automated response capabilities to enable unified security operations and minimize manual intervention. 3. The proposed solution shall be configurable and customizable to meet the Bank's functional, technical, operational, reporting, security, and compliance requirements. 4. The bidder and OEM shall design and implement a secure, scalable, resilient, and future-ready architecture based on the approved requirements, data flows, integrations, and operational needs of the Bank. 5. The bidder and OEM shall prepare and submit the following design documents for Bank approval: a. High-Level Design (HLD), including solution	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner System Design - Activities are to be performed by Respective solution OEM/OEM authorized partner (supported by bidder) 1. The bidder and respective OEM /OEM authorized partner shall be responsible for the end-to-end design, sizing, customization, configuration, integration, implementation, deployment, maintenance, and support of the proposed solution, including coordination with all associated OEMs, service providers, and stakeholders. 2. All proposed NextGEN SOC solutions shall support seamless interoperability, realtime integration, event sharing, correlation, orchestration, and automated response capabilities to enable unified security operations and minimize manual intervention. 3. The proposed solution shall be configurable and customizable to meet the Bank's functional, technical, operational, reporting, security, and compliance requirements. 4. The bidder and OEM/OEM authorized partner shall design and implement a secure, scalable, resilient, and future-ready architecture based on the approved requirements, data flows, integrations, and operational needs of the Bank. 5. The bidder and OEM/OEM authorized partner shall prepare and submit the following design documents for Bank approval: a. High-Level Design (HLD), including solution architecture, deployment architecture, integration architecture, and data flow	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1636	Page 61	7.6.3 Development and Installation - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.6.3	1. All installation, configuration, customization, testing, migration, integration, UAT, GoLive, and related implementation activities shall be performed from the Bank's premises. 2. The bidder and respective OEM shall integrate the proposed solution with the Bank's ITSM, SLA Monitoring, monitoring, logging, authentication, and other enterprise platforms, as required. 3. The bidder and OEM shall coordinate with all relevant third parties, OEMs, service providers, and Bank stakeholders to ensure seamless integration, interoperability, and end-to-end functionality of the proposed solution. 4. The bidder shall provide all required integrations, connectors, parsers, APIs, workflows, playbooks, dashboards, reports, alerts, fine-tuning, customizations, enhancements, and remediation activities necessary for successful operation of the solution throughout the contract period without any additional cost to the Bank. 5. The bidder shall adopt and submit an implementation methodology covering solution deployment, customization, testing, managed services, facility management services, knowledge transfer, and hardware/software installation and configuration activities.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Development and Installation - Activities are to be performed by Respective Solution OEM /OEM authorized partner(supported by bidder) 1. All installation, configuration, customization, testing, migration, integration, UAT, GoLive, and related implementation activities shall be performed from the Bank's premises. 2. The bidder and respective OEM/OEM authorized partner shall integrate the proposed solution with the Bank's ITSM, SLA Monitoring, monitoring, logging, authentication, and other enterprise platforms, as required. 3. The bidder and OEM /OEM authorized partner shall coordinate with all relevant third parties, OEMs, service providers, and Bank stakeholders to ensure seamless integration, interoperability, and end-to-end functionality of the proposed solution. 4. The bidder shall provide all required integrations, connectors, parsers, APIs, workflows, playbooks, dashboards, reports, alerts, fine-tuning, customizations, enhancements, and remediation activities necessary for successful operation of the solution throughout the contract period without any additional cost to the Bank. 5. The bidder shall adopt and submit an implementation methodology covering solution deployment, customization,	No Change, Please be guided by the RFP
1637	Page 62	7.6.4 Documentation - Activities are to be performed by Respective solution OEM (supported by bidder	7.6.4	The bidder and respective OEM shall prepare, maintain, obtain Bank approval/sign-off, and submit all project, technical, operational, security, and administrative documentation associated with the proposed solution. The indicative list of deliverables shall include, but not be limited to, the following: 1. Detailed Project Plan and Implementation Plan 2. Hardware, Software, Infrastructure, and Sizing Specifications 3. High-Level Design (HLD) and Low-Level Design (LLD) Documents 4. Solution Architecture, Deployment Architecture, and Data Flow Documents 5. Secure Configuration Standards, Baseline Hardening Documents, and Security Configuration Guides 6. System, Database, Integration, Troubleshooting, Diagnostics, and Maintenance Documents 7. Testing, Validation, Acceptance, and Go-Live Documents 8. Change Management, Release Management, Problem Management, and Operational Procedures 9. User Management, Access Management, and Role Administration Guides 10. Release Notes, Impact Assessment Matrix, and Dependency Mapping Documents	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Documentation - Activities are to be performed by Respective solution OEM/OEM authorized partner (supported by bidder The bidder and respective OEM shall prepare, maintain, obtain Bank approval/sign-off, and submit all project, technical, operational, security, and administrative documentation associated with the proposed solution. The indicative list of deliverables shall include, but not be limited to, the following: 1. Detailed Project Plan and Implementation Plan 2. Hardware, Software, Infrastructure, and Sizing Specifications 3. High-Level Design (HLD) and Low-Level Design (LLD) Documents 4. Solution Architecture, Deployment Architecture, and Data Flow Documents 5. Secure Configuration Standards, Baseline Hardening Documents, and Security Configuration Guides 6. System, Database, Integration, Troubleshooting, Diagnostics, and Maintenance Documents 7. Testing, Validation, Acceptance, and Go-Live Documents 8. Change Management, Release Management, Problem Management, and Operational Procedures 9. User Management, Access Management, and Role Administration Guides 10. Release Notes, Impact Assessment Matrix, and Dependency	No Change, Please be guided by the RFP
1638	Page 63	7.6.5 Deployment and Go-Live - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.6.5	1. The bidder and respective OEM shall be responsible for deployment of the solution in the production environment, Go-Live planning, implementation, installation, configuration, fine-tuning, migration, stabilization, and hyper care support. 2. The bidder and OEM shall provide onsite support during the hyper care period, monitor solution performance, assist users, conduct training sessions, address issues and defects, implement corrective actions, and recommend operational best practices. 3. The implementation scope shall include deployment planning, migration, testing, validation, issue resolution, user acceptance support, Go-Live execution, and postGo-Live stabilization activities. 4. Prior to Go-Live, the solution shall undergo security validation activities, including VAPT, IS Audit, readiness assessments, identification of security gaps and blind spots, risk remediation, and implementation of recommendations. The Bank or its appointed agency may conduct Continuous Automated Red Teaming, Purple Teaming, security assessments, or other validation exercises as deemed necessary. 5. The bidder and OEM shall conduct performance testing prior to UAT and Go-Live to validate that the	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Deployment and Go-Live - Activities are to be performed by Respective Solution OEM /OEM authorized partner (supported by bidder) 1. The bidder and respective OEM/OEM authorized partner shall be responsible for deployment of the solution in the production environment, Go-Live planning, implementation, installation, configuration, fine-tuning, migration, stabilization, and hyper care support. 2. The bidder and OEM /OEM authorized partner shall provide onsite support during the hyper care period, monitor solution performance, assist users, conduct training sessions, address issues and defects, implement corrective actions, and recommend operational best practices. 3. The implementation scope shall include deployment planning, migration, testing, validation, issue resolution, user acceptance support, Go-Live execution, and postGo-Live stabilization activities. 4. Prior to Go-Live, the solution shall undergo security validation activities, including VAPT, IS Audit, readiness assessments, identification of security gaps and blind spots, risk remediation, and implementation of recommendations. The Bank or its appointed agency may conduct Continuous Automated Red Teaming, Purple Teaming, security assessments,	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1639	Page 64	7.6.6 Testing- Activities are to be performed by Respective solution OEM (supported by bidder)	7.6.6	1. The Bank shall conduct User Acceptance Testing (UAT) to validate that the proposed solution and all associated components, integrations, workflows, reports, dashboards, and functionalities comply with the requirements specified in the RFP, approved FRSM/SRS, and other project documents. 2. The bidder and respective OEM shall confirm completion of all implementations, configuration, customization, integration, migration, and testing activities prior to commencement of UAT and certify that the solution is ready for user validation. 3. The bidder shall provision and maintain dedicated Development, Testing, UAT, and Pre-Production environments throughout the contract period. All software, licenses, and other resources required for such environments shall be included within the bidder's scope without any additional cost to the Bank. 4. Any defects, deviations, vulnerabilities, observations, or non-compliances identified during UAT, security assessments, audits, reviews, or validation exercises shall be rectified by the bidder within the timelines prescribed by the Bank and at no additional cost. 5. The bidder shall maintain appropriate version control, configuration management, change	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Testing- Activities are to be performed by Respective solution OEM/OEM authorized partner (supported by bidder) 1. The Bank shall conduct User Acceptance Testing (UAT) to validate that the proposed solution and all associated components, integrations, workflows, reports, dashboards, and functionalities comply with the requirements specified in the RFP, approved FRSM/SRS, and other project documents. 2. The bidder and respective OEM /OEM authorized partner shall confirm completion of all implementations, configuration, customization, integration, migration, and testing activities prior to commencement of UAT and certify that the solution is ready for user validation. 3. The bidder shall provision and maintain dedicated Development, Testing, UAT, and Pre-Production environments throughout the contract period. All software, licenses, and other resources required for such environments shall be included within the bidder's scope without any additional cost to the Bank. 4. Any defects, deviations, vulnerabilities, observations, or non-compliances identified during UAT, security assessments, audits, reviews, or validation exercises shall be rectified by the bidder within the timelines prescribed by the Bank and at no additional cost.	No Change, Please be guided by the RFP
1640	Page 65	7.6.6.1 Quality Assurance	7.6.6.1	1. Testing Requirements a. The respective OEM shall be responsible for planning, executing, documenting, and successfully completing all testing activities required to validate the functionality, performance, stability, reliability, security, interoperability, and operational readiness of the proposed solution. The bidder shall prepare detailed test plans, test cases, test data, automation scripts (where applicable), entry and exit criteria, test reports, defect logs, root cause analysis reports, workarounds, and remediation plans, and shall obtain the Bank's approval wherever required. 2. Test Preparation The respective OEM shall: a. Prepare the overall testing strategy and methodology for Unit Testing (UT), UAT, Performance Testing, Security Testing, and other applicable tests. b. Establish and maintain the required test environments, infrastructure, software, applications, and test data. c. Prepare, validate, and execute test cases, scripts, and automation frameworks, wherever applicable. d. Define test entry and exit criteria, acceptance criteria, and success parameters. 3. Test Execution The respective OEM shall: a. Execute all approved test cases and scripts. b. Record, track, report, and resolve defects.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: 1. Testing Requirements a. The respective OEM/OEM authorized partner shall be responsible for planning, executing, documenting, and successfully completing all testing activities required to validate the functionality, performance, stability, reliability, security, interoperability, and operational readiness of the proposed solution. The bidder shall prepare detailed test plans, test cases, test data, automation scripts (where applicable), entry and exit criteria, test reports, defect logs, root cause analysis reports, workarounds, and remediation plans, and shall obtain the Bank's approval wherever required. 2. Test Preparation The respective OEM /OEM authorized partner shall: a. Prepare the overall testing strategy and methodology for Unit Testing (UT), UAT, Performance Testing, Security Testing, and other applicable tests. b. Establish and maintain the required test environments, infrastructure, software, applications, and test data. c. Prepare, validate, and execute test cases, scripts, and automation frameworks, wherever applicable. d. Define test entry and exit criteria, acceptance criteria, and success parameters. 3. Test Execution The respective OEM /OEM authorized partner	No Change, Please be guided by the RFP
1641	Page 66	7.6.7 Training- Activities are to be performed by Respective solution OEM (supported by bidder)	7.6.7	7.6.7 Training- Activities are to be performed by Respective solution OEM (supported by bidder) The bidder and respective OEMs shall provide comprehensive product training, knowledge transfer, and certification programs for the Bank's IT and Information Security personnel at no additional cost. All technical and product-specific training shall be delivered by OEM. Upon successful completion of the training programs, the respective OEM shall issue participation and/or certification certificates to the attendees. The bidder shall submit a detailed Training and Certification Plan covering training objectives, curriculum, skill levels, training schedules, participant eligibility, certification pathways, and assessment criteria. The training program shall cover product functionalities, administration, troubleshooting, maintenance, security best practices, automation, advanced threat scenarios, security monitoring and analysis, incident response and investigation, threat detection and hunting, intelligence analysis, new features, upgrades, operational workflows, and relevant industry trends. Bidder along with the OEM should provision the training & certification of the bank's relevant officials from the relevant Cloud service provider where the	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Training- Activities are to be performed by Respective solution OEM /OEM Authorized partner (supported by bidder) The bidder and respective OEMs /OEM authorized partner shall provide comprehensive product training, knowledge transfer, and certification programs for the Bank's IT and Information Security personnel at no additional cost. All technical and product-specific training shall be delivered by OEM/OEM Authorized partner. Upon successful completion of the training programs, the respective OEM /OEM Authorized partner shall issue participation and/or certification certificates to the attendees. The bidder shall submit a detailed Training and Certification Plan covering training objectives, curriculum, skill levels, training schedules, participant eligibility, certification pathways, and assessment criteria. The training program shall cover product functionalities, administration, troubleshooting, maintenance, security best practices, automation, advanced threat scenarios, security monitoring and analysis, incident response and investigation, threat detection and hunting, intelligence analysis, new features, upgrades, operational workflows, and relevant industry trends. Bidder along with the OEM/OEM authorized partner should provision the training & certification of the bank's relevant officials from the relevant	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1642	Page 67	7.6.8 Security requirements - Activities are to be performed by Respective solution OEM (supported by bidder)	7.6.8	1. The bidder and respective OEMs shall comply with the Bank's IT, Information Security, Cyber Security, Data Protection, Privacy, Business Continuity, and related policies, standards, procedures, and guidelines, as shared by the Bank from time to time. The bidder shall be responsible for ensuring the confidentiality, integrity, availability, security, and privacy of the Bank's information assets, systems, applications, and data throughout the contract period. 2. The bidder shall implement and maintain appropriate administrative, technical, physical, and operational controls for protection of data, applications, systems, infrastructure, and associated assets under its custody or management. 3. The bidder shall comply with the Bank's requirements relating to access management, privileged access management, password policies, user administration, data protection, encryption, monitoring, incident management, and security governance. 4. The bidder shall ensure encryption and protection of data at rest, data in transit, and data in use, wherever applicable, using industry-standard security controls and cryptographic mechanisms. All tools, technologies, and controls required to achieve the same shall form part of the proposed solution.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Security requirements - Activities are to be performed by Respective solution OEM/OEM authorized partner (supported by bidder) 1. The bidder and respective OEMs/OEM authorized partner shall comply with the Bank's IT, Information Security, Cyber Security, Data Protection, Privacy, Business Continuity, and related policies, standards, procedures, and guidelines, as shared by the Bank from time to time. The bidder shall be responsible for ensuring the confidentiality, integrity, availability, security, and privacy of the Bank's information assets, systems, applications, and data throughout the contract period. 2. The bidder shall implement and maintain appropriate administrative, technical, physical, and operational controls for protection of data, applications, systems, infrastructure, and associated assets under its custody or management. 3. The bidder shall comply with the Bank's requirements relating to access management, privileged access management, password policies, user administration, data protection, encryption, monitoring, incident management, and security governance. 4. The bidder shall ensure encryption and protection of data at rest, data in transit, and data in use, wherever applicable, using	No Change, Please be guided by the RFP
1643	Page 70	7.7 On-cloud proposed solution OEM Responsibilities	7.6.9	1. The security telemetry received by the OEM Cloud platform will be routed to the dedicated tenant/workspace provisioned for the Bank.	What is the requirement here, is it required to maintain a copy of all cloud data to a local instance /data lake, please clarify, who need to provision this, does bank has this instance available, if not required please remove this ask.	The security telemetry received and processed by the OEM Cloud/SaaS platform shall be logically segregated and maintained within a dedicated tenant/workspace provisioned for the Bank. The dedicated tenant/workspace shall ensure segregation of the Bank's security data, configurations, policies, analytics, alerts, incidents and other Bank-related information from those of other customers.
1644	Page 71	7.10 Data Privacy	7.1 0	Executive Governance and Project Oversight 1. The bidder and each respective OEM shall nominate a senior executive as the Project Sponsor/Project Director responsible for executive governance, stakeholder management, escalation management, strategic oversight, and overall project success. 2. The Project Sponsor, Project Director, and designated senior representatives of the bidder and OEMs shall participate in governance meetings, executive reviews, strategy workshops, and escalation meetings as required by the Bank. An, On quarterly/or as per the frequency defined by bank, executive governance meetings shall be conducted throughout the contract period to review project progress, service delivery, operational performance, security posture, compliance, risks, technology enhancements, and continuous improvement opportunities. 3. The bidder and OEMs shall deploy and maintain adequately skilled, certified, experienced, and qualified resources, together with appropriate backup resources, succession planning, and skill development mechanisms, to ensure uninterrupted 24x7x365 service delivery throughout the contract period.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Executive Governance and Project Oversight 1. The bidder and each respective OEM/OEM authorized partner shall nominate a senior executive as the Project Sponsor/Project Director responsible for executive governance, stakeholder management, escalation management, strategic oversight, and overall project success. 2. The Project Sponsor, Project Director, and designated senior representatives of the bidder and OEMs /OEM authorized partner shall participate in governance meetings, executive reviews, strategy workshops, and escalation meetings as required by the Bank. An, On quarterly/or as per the frequency defined by bank, executive governance meetings shall be conducted throughout the contract period to review project progress, service delivery, operational performance, security posture, compliance, risks, technology enhancements, and continuous improvement opportunities. 3. The bidder and OEMs /OEM Authorized partner shall deploy and maintain adequately skilled, certified, experienced, and qualified resources, together with appropriate backup resources, succession planning, and skill development mechanisms, to ensure uninterrupted 24x7x365 service delivery throughout the contract period. 4. The bidder shall establish and maintain a Bank-approved	Please refer addendum for revised clause
1645	Page 72	7.12 Resource Requirement	7.6.12	7.12.1Implementation Phase • Prior to commencement of implementation, the bidder and respective OEMs shall submit a detailed Resource Deployment Plan for Bank approval identifying proposed onsite and offsite resources, roles, responsibilities, certifications, experience, deployment schedules, and solution-wise allocation. • The bidder shall deploy a dedicated onsite Project Manager throughout the implementation phase and nominate appropriate bidder and OEM resources for each solution, workstream, milestone, and project activity. • Any replacement, redeployment, or modification of approved implementation resources shall require prior written approval from the Bank.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: Implementation Phase • Prior to commencement of implementation, the bidder and respective OEMs /OEM authorized partner shall submit a detailed Resource Deployment Plan for Bank approval identifying proposed onsite and offsite resources, roles, responsibilities, certifications, experience, deployment schedules, and solution-wise allocation. • The bidder shall deploy a dedicated onsite Project Manager throughout the implementation phase and nominate appropriate bidder and OEM /OEM authorized partner resources for each solution, workstream, milestone, and project activity. • Any replacement, redeployment, or modification of approved implementation resources shall require prior written approval from the Bank.	No Change, Please be guided by the RFP
1646	Page 72	7.12.2Operations and Maintenance (O&M) Phase		7.12.2Operations and Maintenance (O&M) Phase • The bidder shall deploy the minimum onsite L1, L2, Project Manager/L3 – Operations, and other resources specified in the RFP and ensure uninterrupted 24x7x365 support through an appropriate shift-based deployment model. • The respective OEMs shall provide subject matter experts from the date of installation throughout the contract period to support operations, troubleshooting, optimization, upgrades, audits, vulnerability remediation, and major incidents. • The bidder shall ensure adequate SME support for timely resolution of incidents, service requests, problems, vulnerabilities, and operational issues.	O & M shall be bidders responsibility pleaase remove OEM from this to maintain right availability and cost Operations and Maintenance (O&M) Phase • The bidder shall deploy the minimum onsite L1, L2, Project Manager/L3 – Operations, and other resources specified in the RFP and ensure uninterrupted 24x7x365 support through an appropriate shift-based deployment model. • The respective bidder shall provide subject matter experts from the date of installation throughout the contract period to support operations, troubleshooting, optimization, upgrades, audits, vulnerability remediation, and major incidents. • The bidder shall ensure adequate SME support for timely resolution of incidents, service requests, problems, vulnerabilities, and operational issues.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1647	Page 73	7.12.3Resource Management and Governance	7.12	OEM Implementation Resources Onsite (Full Time) OEM shall submit a detailed resource deployment plan before commencement of requirement gathering. Any replacement or modification shall require prior Bank approval.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: OEM /OEM authorized partner Implementation Resources Onsite (Full Time) OEM/OEM authorized partner shall submit a detailed resource deployment plan before commencement of requirement gathering. Any replacement or modification shall require prior Bank approval.	No Change, Please be guided by the RFP
1648		7.17 System recovery	1	. In case of disaster, it is the responsibility of the Respective solution OEM along with the bidder to ensure that services remain unaffected and same is up and running from secondary site (DR)	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: . In case of disaster, it is the responsibility of the Respective solution OEM/OEM Authorized partner along with the bidder to ensure that services remain unaffected and same is up and running from secondary site (DR)	No Change, Please be guided by the RFP
1649		7.19 Other In-Scope Services	7.19	7.19.1Other Scope Activity 1. The Respective solution OEM along with the bidder is expected to ensure that all functionalities as mentioned in Appendix 1A: Functional Specification are made available to PSB. 2. The Respective solution OEM along with the bidder is expected to ensure that for the purpose of this RFP, statutory and regulatory changes shall mean any change prescribed by the statutory and regulatory bodies governing/ affecting the banking industry in India viz. Reserve Bank of India, Ministry of Finance, CCIL, NPCI, IBA, SEBI, or any such bodies constituted by the RBI mandating change/s to an existing functionality of the Solution shall be provided to the Bank at no additional cost for the entire contract period. However, any Statutory and Regulatory changes post Go-Live of the respective applications (which are not a part of the existing functionalities) will be on CR basis based on the rates provided in the Bill of Material. 3. The Respective Solution OEM along with the bidder is expected to carry out a requirement study for the functionalities and services required by PSB, to gain understanding of the business requirements. 4. Respective solution OEM along with the bidder	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: 1Other Scope Activity 1. The Respective solution OEM/OEM Authorized partner along with the bidder is expected to ensure that all functionalities as mentioned in Appendix 1A: Functional Specification are made available to PSB. 2. The Respective solution OEM/OEM Authorized partner along with the bidder is expected to ensure that for the purpose of this RFP, statutory and regulatory changes shall mean any change prescribed by the statutory and regulatory bodies governing/ affecting the banking industry in India viz. Reserve Bank of India, Ministry of Finance, CCIL, NPCI, IBA, SEBI, or any such bodies constituted by the RBI mandating change/s to an existing functionality of the Solution shall be provided to the Bank at no additional cost for the entire contract period. However, any Statutory and Regulatory changes post Go-Live of the respective applications (which are not a part of the existing functionalities) will be on CR basis based on the rates provided in the Bill of Material. 3. The Respective Solution OEM/OEM Authorized partner along with the bidder is expected to carry out a requirement study for the functionalities and services required by PSB, to gain understanding of the business requirements. 4. Respective solution OEM /OEM Authorized partner along	Please refer addendum for revised clause
1650		7.19.4DR Setup - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.19.4	DR Setup - Activities are to be performed by Respective Solution OEM (supported by bidder) 1. Respective solution OEM along with the bidder has to ensure that DR setup is ready on the date of Go Live of respective Applications 2. Respective solution OEM along with the bidder should make necessary setup to enable the DR within the agreed timelines. 3. Respective solution OEM along with the bidder should carry out the deployment of the application in DC and DR, UAT as applicable. 4. To ensure proper rollback, Respective solution OEM along with the bidder has to ensure that the old setup at all the locations is as–IS as per the agreed timelines during migration strategy formulation	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner DR Setup - Activities are to be performed by Respective Solution OEM /OEM authorized partner (supported by bidder) 1. Respective solution OEM /OEM Authorized partneralong with the bidder has to ensure that DR setup is ready on the date of Go Live of respective Applications 2. Respective solution OEM/OEM Authorized partner along with the bidder should make necessary setup to enable the DR within the agreed timelines. 3. Respective solution OEM/OEM Authrized partner along with the bidder should carry out the deployment of the application in DC and DR, UAT as applicable. 4. To ensure proper rollback, Respective solution OEM/OEM Authrized partner along with the bidder has to ensure that the old setup at all the locations is as–IS as per the agreed timelines during migration strategy formulation	No Change, Please be guided by the RFP
1651		13 SERVICE LEVELS & PENALTIES	2	2. The bidder and the OEM shall be jointly responsible for the maintenance, configuration, performance, and fault-free operation of the entire supplied infrastructure, including hardware, software, operating systems, databases, and related components, during the warranty, AMC, ATS, and FMS periods, as applicable	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: The bidder and the OEM /OEM authorized partner shall be jointly responsible for the maintenance, configuration, performance, and fault-free operation of the entire supplied infrastructure, including hardware, software, operating systems, databases, and related components, during the warranty, AMC, ATS, and FMS periods, as applicable	No Change, Please be guided by the RFP
1652	Page 159	14.1 Assignment & Subcontracting	1	The selected bidder shall not subcontract/JV/Consortium or permit anyone to perform any of the work, service or other performance required under the contract (excluding Proposed OEM personnels). All bidder's personnel proposed for the bank shall be on bidder's Payroll. Bank will seek relevant documentation from the bidder to validate the same.	To maintain the right availability and overall cost, please rephrase it to OEM/OEM authorized partner: The selected bidder shall not subcontract/JV/Consortium or permit anyone to perform any of the work, service or other performance required under the contract (excluding Proposed OEM /OEM Autorized partner personnels). All bidder's personnel proposed for the bank shall be on bidder's Payroll. Bank will seek relevant documentation from the bidder to validate the same.	No Change, Please be guided by the RFP
1653	Page 30, 34	7.2.1 Deployment Model & HA (TIP) / 7.2.4.1 Deployment Pattern	Table 7.2.1 Sr. 7; Cl. 7.2.4.1(e)	"Threat Intelligence Platform (TIP) - Cloud (SaaS) + Hybrid - Bank Location: Broker/Collector/Integrator: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR" (Table 7.2.1).	Cyble's Threat Intelligence Platform (TIP) is delivered as a fully cloud-native SaaS solution, providing continuous threat-intelligence aggregation, enrichment and distribution to the Bank via API, STIX/TAXII feed and a dedicated web portal, with high availability, geographic resiliency and disaster recovery built into the SaaS platform itself - fully aligned with the SLA, RTO and RPO defined in Section 13. As the TIP's core function requires no packet-level or in-line processing within the Bank's network, Cyble can meet the Bank's continuity requirement for this solution without deploying a broker/collector component on Bank premises. We request the Bank's confirmation that this cloud-native delivery model will be accepted as fully compliant with Table 7.2.1.	Please refer addendum for the revised deployment requirement

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1654	Page 31, 35	7.2.1 Deployment Model & HA (CSPM) / 7.2.4.1 Deployment Pattern	Table 7.2.1 Sr. 11; Cl. 7.2.4.1(i)	"Cloud Security Posture Management (CSPM) - Cloud (SaaS) + Hybrid - Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR" (Table 7.2.1); "...with the required connectors, collectors, agents, enforcers and/or other supporting Bank-side components, if required, deployed at the Bank's DC and DR in N+N Active-Active configuration" (Cl. 7.2.4.1(i)).	Cyble's Cloud Security Posture Management (CSPM) module continuously assesses the Bank's cloud environments through secure, read-only, API-based/cross-account IAM-role integration, with no agent, connector or collector required on Bank premises. This lets Cyble deliver continuous, real-time cloud security posture monitoring with high availability and resilience built natively into the SaaS platform, fully meeting the Bank's SLA, RTO and RPO requirements under Section 13. This is consistent with the qualifying language "if required" already present in Cl. 7.2.4.1(i). We request the Bank's confirmation that this API-integrated, cloud-native delivery model will be accepted as compliant.	Please refer addendum for the revised clause
1655	Page 55-56	7.4.3 Attack Surface Management	Cl. 7.4.3	"Discovery of internet-facing and internal assets... The proposed solution shall provide AI-enabled Attack Surface Management (ASM) capabilities for continuous discovery... of the organization's external attack surface, including known and unknown internet-facing assets."	Cyble's Attack Surface Management (ASM) capability provides continuous, AI-enabled discovery, monitoring and risk-prioritization of the Bank's entire external attack surface - internet-facing assets, exposed services, domains, cloud assets and shadow IT - using external/passive reconnaissance together with Bank-shared asset inventories (IP ranges, domains, cloud accounts), with no agent or appliance required inside the Bank's network, consistent with the offsite Managed Service model in Section 7.2.2. This gives the Bank a complete outside-in exposure view from Day 1. We request the Bank's confirmation that this externally-led, agentless approach satisfies Cl. 7.4.3.	Bank is looking for external attack surface management
1656	Page 55	7.4.5 Anti-Phishing	Cl. 7.4.5	"...offsite continuous anti-phishing monitoring and response services for detection, analysis for phishing attacks targeting the Bank, its employees, customers, executives, digital assets, domains, and online channels."	Cyble is fully equipped to deliver continuous, 24x7 Anti-Phishing monitoring across the Bank's domains, executives and digital channels from Day 1 of the engagement, scaling seamlessly as the Bank's digital footprint grows, with no additional infrastructure required from the Bank. To finalise the onboarding plan, we request the Bank share the number of primary/registered domains, sub-domains, executive/VIP identities and customer-facing digital channels to be covered at contract commencement, so Cyble can confirm precise sizing against this scope.	Please refer to the relevant Addendum for updated specfications
1657	Page 57	7.4.6 Dark Web Monitoring	Cl. 7.4.6	"...offsite, tool-based continuous dark web and cyber threat exposure monitoring services... across the surface web, deep web, dark web, underground forums, messaging platforms, and data leak repositories."	Cyble's Dark Web & Cybercrime Monitoring capability continuously covers the surface web, deep web, dark web, underground forums, messaging platforms and data-leak repositories, and can begin protecting the Bank's specified identities, brand keywords and domains immediately upon contract signature. To tailor this coverage precisely, we request the Bank share the initial monitoring scope (employee/executive identities, brand keywords, domains and relevant data categories) so Cyble can confirm sizing and reporting cadence.	Details shall be shared with succesful bidder
1658	Page 57	7.4.7 Threat Intelligence Feed	Cl. 7.4.7(l)	"Provision of threat intelligence through a centralized portal/dashboard and/or machine-readable feeds."	Cyble's Threat Intelligence Feed is delivered through both a centralized portal/dashboard and machine-readable, standards-based feeds (STIX/TAXII, MISP-compatible formats and API), enabling seamless integration with the Bank's existing or future security stack whenever required. We confirm this dual delivery model - portal-based consumption plus machine-readable feed/API - and request the Bank's confirmation that it satisfies Cl. 7.4.7.	No Change, Please be guided by the RFP
1659	Page 57-58	7.4.8 Threat Hunting Services	Cl. 7.4.8(m)	"The threat hunting service shall be delivered remotely/offsite using secure and mutually agreed mechanisms for accessing relevant logs, telemetry, security tools, and data made available by the Bank."	Cyble can deliver proactive, intelligence-driven Threat Hunting entirely offsite - correlating curated external threat intelligence (IOCs, IOAs, TTPs, threat-actor and campaign intelligence) against Bank-shared context, supplemented by secure, mutually agreed read-only access to relevant Bank telemetry for validation and deeper investigation as needed - fully consistent with the remote/offsite delivery model mandated in Cl. 7.4.8(m). We request the Bank's confirmation that this intelligence-led hunting model, combined with agreed read-only telemetry access, meets the Bank's requirement.	No Change, Please be guided by the RFP
1660	Page 58	7.4.9 Brand Protection and Monitoring	Cl. 7.4.9(j)	"Takedown coordination with relevant registrars, hosting providers, platforms, application stores, social media platforms, and other relevant entities, wherever applicable."	Cyble's Brand Reputation Monitoring capability continuously identifies brand impersonation, typosquatting, phishing/fraudulent websites, fraudulent mobile apps and social-media impersonation, and actively coordinates takedown requests with registrars, hosting providers, app stores and social platforms on the Bank's behalf under a standard authorisation executed at contract signature - delivering a fully managed, end-to-end takedown process with minimal effort required from the Bank's team. We request the Bank's confirmation that this bidder-led takedown coordination model satisfies Cl. 7.4.9(j).	Please refer addendum for revised clause
1661	Page 256	16.21 Annexure 21: Sizing/Volumetrics (gap for Offsite Services)	Annexure 21, Sizing table	Annexure 21's sizing table provides explicit volumetrics (EPS, endpoint counts, IPs, VPCs, etc.) for the 14 solutions under Section 7.3, but no equivalent executive/VIP count is specified for the offsite services that monitor executive exposure (Anti-Phishing - Cl. 7.4.5, Dark Web Monitoring - Cl. 7.4.6, Brand Protection - Cl. 7.4.9).	Cyble's Executive Monitoring and Digital Risk Protection capabilities can protect any number of the Bank's executives/VIPs from Day 1, with coverage scaled precisely to the Bank's requirement across Anti-Phishing, Dark Web Monitoring and Brand Protection. To finalise sizing, we request the Bank confirm the number of executives/VIPs (e.g., Board members, CXOs, senior management) to be brought under continuous monitoring at contract commencement.	Please refer to the relevant Addendum for updated specfications
1662	Page 256	16.21 Annexure 21: Sizing/Volumetrics (gap for Offsite Services)	Annexure 21, Sizing table	As above - no domain/sub-domain count is specified for the offsite services that monitor the Bank's external digital footprint (Attack Surface Management - Cl. 7.4.3, Anti-Phishing - Cl. 7.4.5, Brand Protection - Cl. 7.4.9).	Cyble can bring any number of the Bank's domains and sub-domains under continuous monitoring across Attack Surface Management, Anti-Phishing and Brand Protection from Day 1. To finalise sizing, we request the Bank confirm the number of primary domains and sub-domains to be monitored at contract commencement, and the expected annual growth in this count.	details shall be shared with successful bidder

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1663	Page 54	7.4 Functional Requirement - Services (Offsite Services)	Cl. 7.4(d)	"The Bidder shall implement appropriate security controls, including data masking or tokenization for sensitive data, Role-Based Access Control (RBAC), Just-in-Time (JIT) privileged access, and comprehensive audit logging for all services delivered under this RFP." - no named-user/license count is specified for platform/dashboard access to the 9 offsite services.	Cyble's platform can be provisioned for any number of the Bank's analysts, CISO-office and compliance stakeholders who need dashboard access to the offsite services, with full role-based access control as required under Cl. 7.4(d). To size the commercial bid precisely, we request the Bank confirm the number of named analyst/console user licenses required for the Bank's teams to access Cyble's platform and reporting for the proposed offsite services.	details shall be shared with successful bidder
1664	Page 55, 58	7.4.5 Anti-Phishing / 7.4.9 Brand Protection and Monitoring	Cl. 7.4.5; Cl. 7.4.9(j)	Neither clause, nor Annexure 21, specifies an expected volume of takedown actions per month/year for phishing sites, fraudulent domains, or fake social media/mobile app listings.	Cyble is fully equipped to execute takedown actions at whatever volume the Bank's threat exposure requires. To align commercial terms precisely with the Bank's risk profile, we request the Bank confirm the estimated number of takedown actions (phishing sites, fraudulent domains, fake social media/mobile app listings) expected per month under Anti-Phishing and Brand Protection.	Please refer to the relevant Addendum for updated specfications
1665	pg. 84-85	Section: 7.15 NextGEN SOC Operations	SOC Monitoring, Incident Investigation & Operations Management	Bidder to perform end-to-end investigation of security alerts and incidents, including triage, enrichment, correlation, impact assessment, response coordination, and closure.	We request the Bank to provide the current average monthly security incident count, including the number of Critical, High, Medium, and Low incidents, along with the approximate True Positive (TP) and False Positive (FP) count, for accurate SOC planning and effort estimation	details shall be shared with successful bidder
1666	pg. 42	7.3.2 SOAR	7.3.2.2 Key Deliverables	Integration with SIEM, XDR, NDR, UEBA, TIP, ITSM, IAM/PAM, network, endpoint, cloud and other relevant security solutions	We request the Bank to provide the name and version of the existing ITSM/ticketing tool to assess the ease of integration with the proposed SIEM solution.	ITSM - Manage Engine
1667	pg. 257	16.21.1	Current IT assets	Current assets description	We request the Bank to provide the detailed list of log sources type along with OEM name,that need to be integrated with the proposed SIEM solution for accurate sizing and implementation planning.	details shall be shared with successful bidder
1668	pg. 40	7.3.1.1	Point 6 (l)	Support collection of logs and telemetry from third-party systems and services	We request the Bank to confirm whether any traditional/legacy third-party devices or applications are in scope for integration. The integration feasibility and effort may vary depending on the product make/model and availability of OEM-supported connectors or APIs	Details shall be shared with the successful bidder
1669	pg. 74	7.12.3	L2 Security Resources	Minimum 5 years' experience, minimum two OEM/security certifications, and SOC experience in two or more PSU/PSE/Government/BFSI/Regulatory organizations	We request the Bank to consider relaxing the L2 resource criteria by allowing a minimum of 3 years of relevant SOC/cybersecurity experience and one OEM/security certification. We also request relaxation of the PSU/PSE/Government/BFSI specific experience requirement, as the current criteria significantly restrict the availability of qualified resources despite candidates possessing relevant SOC operational experience.	No Change, Please be guided by the RFP
1670	pg. 74	7.12.3	L3 / Project Manager - Operations	Minimum 8 years' experience, minimum two OEM/security certifications, and experience in managing at least two SOC engagements in PSU/PSE/Government/BFSI/Regulatory/Fortune 500 organizations	We respectfully request that the eligibility criteria be revised to allow bidders to demonstrate experience where the proposed solutions have been supplied or installed, or maintained, rather than requiring evidence that the solutions have been supplied, installed, and maintained cumulatively. This amendment would better reflect the diverse engagement models under which organizations deliver and support enterprise-scale technology solutions. Additionally, we request the inclusion of Public Private Partnership (PPP) organizations, as well as organizations from the Technology, Media, and Telecommunications (TMT) sector and the Manufacturing sector, alongside the currently specified sectors. These industries are highly technology-dependent and operate complex, large-scale enterprise environments comparable in scope, scale, and criticality to those currently considered under the eligibility criteria. Expanding the eligible sectors in this manner would encourage broader participation from qualified bidders with relevant experience in deploying, managing, and supporting complex enterprise-scale technology environments, thereby enhancing competition and enabling the Authority to benefit from a wider pool of capable service providers.	No Change, Please be guided by the RFP
1671	pg. 76	7.12.5	Point 7	Resource Replacement and Knowledge Transfer Period	We request the Bank to consider reducing the mandatory knowledge transfer period during resource replacement, as the proposed timelines may be difficult to achieve in cases of unforeseen circumstances. The bidder shall ensure adequate transition and knowledge transfer through suitable replacement resources.	No Change, Please be guided by the RFP
1672	pg. 36 - 38	7.2.4.3	Storage and Retention Requirements	SIEM Log Retention & Long-Term Storage	We request the Bank to clarify the hot and cold storage requirements for SIEM logs. Further, for the 5-year log retention requirement, please confirm whether the logs are required to remain online and searchable throughout the retention period or can be archived and restored on demand when required.	Please refer addendum for revised clause
1673	pg. 143-144	13.1 Service Level Agreement	Incident Classification & Response Time	Response Time: 15 Minutes for Critical/High, Medium, and Low Severity Incidents	We request the Bank to consider revising the response SLA based on incident severity, in line with industry best practices and operational prioritization, as follows: Critical/High Severity: 15 Minutes Medium Severity: 30 Minutes Low Severity: 60 Minutes	No Change, Please be guided by the RFP
1674	pg. 143-144	13.1 Service Level Agreement	Incident Classification & Response Time	Incident response, escalation, and resolution management.	Request bank to note that the bidder's scope is limited to incident detection, analysis, reporting, and escalation to the concerned Bank's teams for necessary action. As per generally accepted industry practices for SOC/MSP engagements, incident remediation and resolution activities are typically performed by the respective asset, application, or system owners.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1675	pg. 49-52	SIEM Implementation & Operations	Use Cases, Correlation Rules, Dashboards and Reports	SIEM onboarding, use case development, tuning and monitoring	We request the Bank to clarify whether migration of existing SIEM correlation rules, use cases, dashboards, reports, and integrations is in scope. If yes, kindly provide the approximate count to enable accurate effort estimation and implementation planning.	Yes, the existing SIEM/SOC platform is operational and will be replaced under this RFP. No historical data migration from the existing SIEM is envisaged. The existing SIEM/SOC infrastructure and solution shall be operated and maintained by the bidder on an "as-is, where-is" basis during the parallel-run period, as required for compliance, at no additional cost to the Bank.
1676	pg. 42-44	7.3.2 SOAR	SOAR Implementation & Automation	Playbook development, orchestration and automation	We request the Bank to provide the expected number of SOAR playbooks to be implemented during the initial rollout and the estimated number of additional playbooks expected during the contract period.	No Change, Please be guided by the RFP
1677	pg. 53-57	7.4 Threat Intelligence Services	Threat Intelligence Integration & Enrichment	Integration of threat intelligence with SOC/SIEM ecosystem	We request the Bank to confirm whether any existing Threat Intelligence feeds/subscriptions need to be integrated with the proposed solution. If yes, kindly provide the details.	No Change, Please be guided by the RFP
1678	pg. 258-259	16.21.2 Volumetrics - Solution-wise Requirements	XDR Solution for 12,000 Users scalable to 14,000	XDR Sizing	We request the Bank to provide the operating system-wise endpoint count in scope for the proposed XDR solution, including Windows, Linux, Unix, macOS, and other endpoint categories, for accurate sizing, licensing, and implementation planning.	No Change, Please be guided by the RFP
1679	pg. 157	13.2 Penalties	Maximum Penalty Cap	Total penalties under LD & SLA shall be subject to a maximum of 10% of the overall contract value	We request the Bank to consider revising the maximum cumulative penalty cap from 10% of the overall contract value to 3% of the contract value	No Change, Please be guided by the RFP
1680	pg. 143-157	13.1 Service Level Agreement & 13.2 Penalties	SLA Measurement, Penalties and Service Credits	SLA Parameters, Penalty Framework and Applicability	We request the Bank to note that the detailed SLA parameters and penalty framework shall be mutually discussed and finalized during the contract signing stage.	No Change, Please be guided by the RFP
1681	Pg. 49	7.3.11		Cloud Security (CSPM) Tool	The CSPM scope describes a single-pane view covering cloud assets, workloads, identities, applications, containers and AI services, while Sections 7.3.12 and 7.3.13 separately prescribe CNAPP and CWPP. Please clarify the exact functional boundary and ownership of requirements among CSPM, CNAPP and CWPP, and confirm that duplicate licensing, scanning, telemetry ingestion and storage will not be required for the same cloud resource.	No Change, Please be guided by the RFP
1682	pg. 50	7.3.11.1 and 7.3.11.2		CSPM modules, integrations and deliverables	Please provide the cloud platforms currently in scope and expected during the contract period, including public cloud providers, private cloud platforms, SaaS services, accounts/subscriptions/projects, regions and organization/management-group hierarchy, so that connectors, API permissions, licensing and implementation effort can be accurately sized.	No Change, Please be guided by the RFP, Details shall be shared with the successful bidder
1683	pg. 260	16.21.2, Item 13		CSPM volumetrics: 'At least 20 VMs (VPCs)'	The volumetric uses the expression '20 VMs (VPCs)', although VMs and VPCs are different licensing and sizing units. Please clarify whether the requirement is 20 VPCs/VNets, 20 VMs, or both, and provide the expected number of cloud accounts/subscriptions/projects and anticipated annual growth.	Details shall be shared with successful bidder
1684	pg. 50	7.3.11.1(3-9)		CSPM posture assessment, drift and reporting	Please confirm the mandatory compliance frameworks and benchmarks to be enabled at Go-Live, such as RBI requirements, CERT-In, CIS benchmarks, NIST, ISO 27001, PCI DSS and Bank-specific policies, together with the required assessment frequency, report frequency and number of custom policies/controls expected.	No Change, Please be guided by the RFP
1685	pg. 51	7.3.12		CNAPP platform scope	Please confirm whether a single integrated CNAPP platform may be proposed to deliver CSPM, CIEM, IaC, SCA, secrets, container/Kubernetes, API risk, attack-path and workload capabilities, while still providing separate compliance mapping, deliverables and commercial line items for CSPM, CNAPP and CWPP.	No Change, Please be guided by the RFP
1686	pg. 51	7.3.12.1(3)		SCA, IaC and secrets scanning	Please provide the expected number and types of source-code repositories, IaC repositories, CI/CD tools, container registries, programming languages and IaC frameworks to be onboarded. Also confirm whether scanning must be unlimited or whether a defined repository/user/scan volume will be provided for commercial sizing.	No Change, Please be guided by the RFP
1687	pg. 51	7.3.12.2(3-4)		Source-Code Security Assessment and SCA reports	Section 7.3.12 requires a Source-Code Security Assessment Report and SCA Report, while Section 7.3.10 separately procures the Application Security Testing Tool. Please clarify whether CNAPP is expected to perform SAST, or only SCA, secrets and IaC scanning, to avoid duplication with the AST solution.	No Change, Please be guided by the RFP
1688	pg. 51	7.3.12.1(4) and 7.3.12.2(8)		API security findings and API Security Assessment Report	Please clarify whether CNAPP must include active API discovery/testing and runtime API protection, or only ingest and correlate API findings from the Application Security Testing/API security solution. Please also provide the expected number of APIs and API gateways if native API assessment is mandatory.	No Change, Please be guided by the RFP
1689	pg. 51	7.3.12.2(10)		CI/CD & DevSecOps Integration	Please provide the existing and planned CI/CD, source-code management, artifact repository, container registry and ticketing platforms, including whether production integration credentials and test pipelines will be made available during implementation and UAT.	No Change, Please be guided by the RFP, Details shall be shared with the successful bidder
1690	pg. 261	16.21.2, Item 15		CWPP volumetrics: 20 VPCs/VNets and 100 VMs	Please confirm the commercial licensing unit for CWPP and whether the 100-VM count includes autoscaling instances, Kubernetes worker nodes and on-premises servers. Please specify how temporary/ephemeral workloads are to be counted and billed.	No Change, Please be guided by the RFP, Details shall be shared with the successful bidder
1691	pg. 36	7.2.4.3(1)(a-e)		Long-term archival, ingress/egress and restoration	Please clarify the required export format, frequency and transfer mechanism for long-term archival to the Bank, and confirm whether restoration means re-import into the native SaaS platform or making exported data readable/searchable through a Bank-designated platform. Please provide the applicable RTO for such restoration.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1692	pg. 52	7.3.13.1(14)		Integration with SIEM, SOAR and XDR	Please provide the expected integration scope and data direction for CSPM/CNAPP/CWPP with SIEM, SOAR, XDR, ITSM and CMDB.	No Change, Please be guided by the RFP
1693	pg. 117	10.2, Eligibility Criterion 22		Separate credentials for CNAPP, CWPP and CTEM	The RFP requires separate credentials for CNAPP, CWPP and CTEM and later states that each solution must be demonstrated as a standalone deployment rather than a feature of another solution. Since these capabilities are commonly delivered through unified platforms, please confirm whether a single client deployment and contract can substantiate multiple categories when the supporting documents clearly evidence that each required capability was licensed, implemented and used in production.	No Change, Please be guided by the RFP
1694	27, 58-59	7.1, 7.5	Key Implementation Responsibilities	Implementation activities to be performed by OEM supported by Bidder	Kindly confirm whether implementation experience demonstrated through OEM-led deployments under bidder project governance shall be considered for bidder eligibility evaluation.	No Change, Please be guided by the RFP
1695	60-67	7.6	OEM Responsibilities	Requirement Analysis, Design, Installation, Testing, Go-Live to be performed by OEM	Please clarify whether OEM implementation resources may be deployed remotely for part of the implementation activities or whether 100% onsite deployment is mandatory.	No Change, Please be guided by the RFP
1696	73-75	7.12.4	Minimum Resource Count Deployment	Minimum L1, L2 and L3 resource deployment	Kindly confirm whether the prescribed manpower count is a contractual minimum mandatory deployment throughout the contract period or an indicative staffing guideline.	The manpower requirement provided in the RFP are minimum mandatory requirement i.e to be provided by the bidder.
1697	75	7.12.4	Resource Deployment	Resource sharing across technologies	Please confirm whether L1, L2 and L3 resources can support multiple security technologies simultaneously, provided SLA requirements are met.	No Change, Please be guided by the RFP
1698	29-31, 257-261	7.2.1, Annexure 21	Solution Deployment & Volumetrics	SIEM sizing of 50,000 EPS scalable to 75,000 EPS	Kindly clarify whether the quoted EPS requirement represents total enterprise log ingestion or only the logs to be onboarded under this project scope.	No Change, Please be guided by the RFP
1699	29-35	7.2	Deployment Model	Individual solutions listed separately	Can bidders propose an integrated platform offering multiple capabilities such as SIEM, SOAR, UEBA, XDR and TIP, provided all functional requirements are met?	No Change, Please be guided by the RFP
1700	95-96	7.19.3	Security Management	Multiple security tools integration	Please confirm whether APIs and native connectors from proposed integrated platforms will satisfy individual integration requirements envisaged under the RFP.	No Change, Please be guided by the RFP
1701	95	7.19.2	Transition Management	Takeover of existing SOC operations from 01.05.2027	Request sharing of existing SOC architecture, currently deployed tools, OEMs, current log volumes and incumbent support arrangements for accurate effort estimation.	Details shall be shared with the successful bidder
1702	101-119	10.2	Eligibility Evaluation Criteria	SIEM and security solution deployment criteria	Kindly confirm whether cloud-hosted or SaaS-based deployments shall be considered equivalent to on-premises deployments for eligibility qualification.	No Change, Please be guided by the RFP
1703	110	10.2 Clause 19	OEM Eligibility	SIEM OEM reference requirement	Kindly clarify whether global references with deployment in India shall qualify for OEM eligibility requirements.	No Change, Please be guided by the RFP
1704	112-120	10.2 Clauses 20-23	OEM Experience	BFSI implementation requirements	Can a single client reference showcasing multiple technologies be used to meet eligibility criteria for multiple solution categories?	No Change, Please be guided by the RFP Note: - Experience of solutions can be shown in single /multiple Clients/ work orders meeting the above criteria
1705	123-126	10.2 Clause 25	Functional Compliance	Minimum 85% compliance score	Please clarify whether requirements marked as "C" (Customization) must be available before technical evaluation or can be delivered before UAT as stated in the RFP.	No Change, Please be guided by the RFP
1706	137-140	12	Payment Terms	SaaS subscription payment	Please clarify whether annual subscription costs for cloud-hosted solutions shall be paid annually in advance or linked to project milestones.	No Change, Please be guided by the RFP
1707	146-158	13	SLA & Penalties	SLA and LD calculations	Kindly confirm whether SLA penalties are cumulative across all technologies and services or capped separately for each technology/service.	No Change, Please be guided by the RFP RFP Clause 13.2 - For the purpose of this RFP, the total penalties as per LD & SLA will be subject to a maximum of 10% of the overall contract value
1708	87-88	7.16	OEM Assessment & Architecture Review	Annual OEM reviews	Please clarify whether OEM assessment and architecture review activities may be conducted remotely through virtual workshops and reports.	No Change, Please be guided by the RFP
1709	66	7.6.7	Training Requirements	Training and certification of 15 officials	Kindly clarify whether OEM-authorized online training and certification programs are acceptable for compliance with the training requirement.	Please refer addendum for revised clause
1710	68-69	7.7	Cloud Solution OEM Responsibilities	Data residency requirement	Please confirm whether cloud service providers operating India data centers are acceptable, provided all Bank data remains within India.	No Change, Please be guided by the RFP
1711	26-28	7.1	Scope and Objectives	NextGen SOC Technologies	Kindly clarify whether only commercial/OEM-supported products are acceptable or whether enterprise-supported open-source solutions may also be proposed where they satisfy all functional, support and SLA requirements.	No Change, Please be guided by the RFP
1712	54-58	7.4	Functional Requirement - Services	Managed Security Services	The RFP specifies outcomes and service requirements for BAS, CART, ASM, Threat Intelligence, Threat Hunting, Dark Web Monitoring and Brand Monitoring. Kindly clarify whether bidders may leverage commercial OEM products, enterprise-supported open-source solutions and bidder-owned proprietary platforms, methodologies, automation frameworks and managed service capabilities to deliver these services, provided all functional requirements, deliverables, reporting obligations and SLA commitments are met.	Bidder to propose the managed OEM Services complying with the requirement mentioned in the RFP and complying with the PQ and TQ requirement for each product/services
1713	55	7.4.2	Continuous Automated Red Teaming	Adversary Emulation	Please clarify whether the requirement is limited to automated red teaming tooling or whether manual red team exercises are also expected periodically during the contract period.	Bank is looking for Continuous Automated red teaming services. Bank is not looking for Playbook creation as a a part of the CART. Clarification:- The solution shall support continuous adversary emulation using realistic, threat-informed and multi-stage attack scenarios, including scenarios based on relevant threat actors and their Tactics, Techniques and Procedures (TTPs), mapped to the MITRE ATT&CK framework.
1714	55	7.4.1 & 7.4.2	BAS & Continuous Automated Red Teaming	BAS/CART Services	Kindly confirm whether BAS and Continuous Automated Red Teaming services are expected to include exploitation activities in production environments or only validation and simulation activities.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1715	47-48	7.3.8, 7.3.9	Vulnerability Management & ITDR	Vulnerability Lifecycle Management	Does the bidder need to perform vulnerability assessment activities or only manage vulnerabilities identified through the proposed platform/tooling?	Bidder is required to maintain, manage and run the VA& VLM tool for the duration of the contract
1716	47-48	7.3.8	Vulnerability Assessment & Vulnerability Lifecycle Management	Assessment Scope	Kindly clarify whether infrastructure VAPT, web application VAPT, mobile application VAPT, API security assessment and cloud security assessments are in scope under this RFP.	No Change, Please be guided by the RFP
1717	48-49	7.3.10	Application Security Testing Tool	SAST & DAST	Is the bidder expected to perform application security assessments and remediation validation, or only provide and operate the AST platform?	Please be guided by the RFP, Bidder to perform both security assessments and remediation validation
1718	48-49	7.3.10	Application Security Testing Tool	API & Mobile Security	Kindly confirm the number of web applications, mobile applications and APIs expected to be onboarded under the AST solution during the contract period.	The bidder shall size based on the volumetrics provided in the RFP, Further details shall be shared with the successful bidder.
1719	84-85	7.15	NextGen SOC Operations	Incident Handling	Please clarify whether Incident Response activities are limited to detection, triage and coordination, or whether the bidder is expected to provide full Incident Response and Digital Forensics services.	No Change, Please be guided by the RFP
1720	84-85	7.15	NextGen SOC Operations	Security Incident Management	In case Incident Response support is required, kindly confirm whether onsite incident response resources are expected or remote support from OEM/bidder SMEs is acceptable.	No Change, Please be guided by the RFP
1721	26-28, 84-85	7.1, 7.15	AI Security Requirements	AI-related Security Monitoring	The RFP references AI threats, AI-enabled attacks and AI security monitoring. Kindly clarify whether explicit AI Security Assessments of Bank-developed or third-party AI/GenAI applications are in scope. Kindly clarify whether the requirement includes governance and security assessment of AI/LLM applications or is limited to logging and threat detection use cases.	Reference is not part of this RFP
1722	49-53	7.3.11 to 7.3.14	CSPM, CNAPP, CWPP & CTEM	Cloud Security Assessments	Kindly confirm whether periodic cloud security configuration reviews and cloud architecture reviews are expected to be delivered as managed services.	No Change, Please be guided by the RFP
1723	67-69	7.6.8, 7.7	Security & Cloud Responsibilities	Configuration Baseline Reviews	Please clarify whether secure configuration reviews, hardening reviews and benchmark validation against CIS/NIST standards are expected periodically and whether these activities are part of managed services.	No Change, Please be guided by the RFP
1724	77-83	7.13	Facilities Management	Monthly Gap Analysis & Reviews	Kindly clarify whether the bidder is expected to conduct independent security assessments and configuration reviews on a periodic basis or only manage OEM tooling outputs.	Please be guided by the RFP
1725	63-65	7.6.5 & 7.6.6	Testing & Security Validation	Security Testing Before Go-Live	The RFP mandates VAPT, Purple Teaming and security validation before Go-Live. Please clarify whether these assessments shall be conducted by the bidder or independently by the Bank.	No Change, Please be guided by the RFP
1726	63-65	7.6.5	Security Validation	VAPT & Purple Teaming	If the bidder is expected to perform these assessments, kindly provide volumetrics for infrastructure, applications, APIs, mobile applications and cloud environments to be tested.	Details shall be shared with successful bidder
1727	77-83	7.13	Facilities Management	Vulnerability Closure Requirements	Kindly clarify whether remediation activities are expected to be executed by the bidder or recommendations and validation of remediation performed by Bank/application owners is sufficient.	For the Bidder's proposed solution and infrastructure, the Bidder/OEM shall be responsible for remediation of vulnerabilities identified in the proposed solution/infrastructure and shall ensure their closure. For the Bank's existing applications, systems and infrastructure, the Bidder/OEM shall provide remediation recommendations and perform remediation validation/re-scanning, while the actual remediation shall be carried out by the respective Bank/application owners.
1728	83-87	7.14 & 7.15	DR Drill & SOC Operations	Cyber Drills and Tabletop Exercises	Please confirm the expected number of cyber drills, tabletop exercises, threat simulations and incident response exercises to be conducted annually under the contract.	Please refer section 7.13: Facilities Management, Point 9.
1729	27, 58-67, 103-119	7.5, 7.6, 10.2	Bidder & OEM Responsibilities	Solution implementation and managed operations	Since the RFP explicitly states that implementation activities are to be performed by the respective OEMs and operational activities are to be managed by the bidder, kindly clarify whether bidders may demonstrate managed services and operational experience while OEMs may independently demonstrate implementation and deployment experience for the proposed technologies.	No Change, Please be guided by the RFP
1730	103-108	10.2 Clause 7 & 8	SIEM and Security Tool Experience	Bidder implementation experience	Kindly confirm whether implementation references of the proposed OEM may be considered for qualification where the OEM is contractually responsible for implementation activities and the bidder is responsible for project governance, operations and managed services.	No Change, Please be guided by the RFP
1731	103-108	10.2	Eligibility Criteria	Security solution implementation experience	Kindly clarify whether managed security operations experience involving operation and management of SIEM, SOAR, XDR, UEBA, TIP and related technologies shall be considered equivalent to implementation experience for qualification purposes.	No Change, Please be guided by the RFP
1732	105-119	10.2	Technology Experience	Multiple technology deployment references	Kindly confirm whether technology experience may be demonstrated collectively through the bidder, OEM and bidder group entities/affiliates, subject to submission of documentary evidence and project responsibilities.	No Change, Please be guided by the RFP
1733	169	15.2	APPENDIX 1B: Technical Compliance Sheet (IT Infrastructure) - Load balancer	34.OEM should have TAC & R&D facility in INDIA. The proposed solution should be up and running in PSU/PSE/Govt. Organization within the last 5 years	International OEM shall be acceptable. Solution running internationally shall also be acceptable. Please consider international supply also for maximum participation.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1734	163-165		Bidder shall indemnify the Bank against all losses, damages, claims, costs, legal expenses, third-party claims, IP infringement and regulatory actions.	Broad indemnity with no explicit financial cap.	Modify: Bidder's aggregate indemnity liability shall be capped at 100% of Contract Value except for fraud, willful misconduct and proven IP infringement.	No Change, Please be guided by the RFP
1735	165		Limitation of liability excludes IP infringement, confidentiality breach, gross negligence and regulatory fines.	Major liabilities carved out from liability cap.	Modify: Liability cap to apply to all claims except fraud and willful misconduct. Regulatory penalties and confidentiality breaches should be subject to a separate negotiated cap.	No Change, Please be guided by the RFP
1736	163-165		Includes legal expenses, reputation loss and third-party claims.	Exposure to consequential and indirect damages.	Add: Neither party shall be liable for indirect, incidental, special, punitive or consequential damages, including loss of profits or reputation.	No Change, Please be guided by the RFP, Clause 14.21 – Limitation of Liability.
1737	166		Bank may cancel unexecuted portion of PO for delay, breach or performance issues.	Broad unilateral cancellation rights.	Modify: Provide minimum 30-day cure period and mutual dispute resolution before cancellation.	No Change, Please be guided by the RFP
1738	168		Bidder must support transition and successor vendor at no additional cost.	Unlimited transition obligation.	Modify: Transition support limited to 30 days and billable at mutually agreed rates.	No Change, Please be guided by the RFP
1739	129-130		Bank may increase/decrease quantities by ±25% at same rates.	Significant commercial exposure without repricing.	Modify: Any variation exceeding ±10% shall be subject to commercial renegotiation and mutually agreed delivery timelines.	No Change, Please be guided by the RFP
1740	137		No advance payment.	Bidder funds entire implementation and procurement.	Request mobilization advance of 10% against Bank Guarantee or milestone payment upon contract signing.	No Change, Please be guided by the RFP
1741	158		Bank may retain up to 15% of monthly payout against SLA compliance.	Cash-flow impact and double recovery risk.	Clarify that ARA and SLA penalties are not cumulative and total deductions shall be capped.	No Change, Please be guided by the RFP
1742	155-160		Multiple penalties for outages, audit observations, regulatory delays and support lapses.	Overlapping penalty regime.	Modify: Aggregate SLA penalties shall not exceed 10% of annual contract value.	No Change, Please be guided by the RFP RFP Clause 13.2 - For the purpose of this RFP, the total penalties as per LD & SLA will be subject to a maximum of 10% of the overall contract value
1743	142 / 156		Additional penalties for customer-facing outages and delayed closure of observations.	Potential multiple penalties for same incident.	Clarify that only one penalty shall apply for a single root-cause event.	No Change, Please be guided by the RFP
1744	168		Bank/regulators may audit records and premises as often as required.	Unlimited audit frequency.	Modify: Maximum one audit per year except regulatory audits. Require 15 business days' notice.	No Change, Please be guided by the RFP
1745	71 / 128+		Bidder responsible for confidentiality and DPDP compliance.	Unlimited exposure for data incidents.	Modify: Liability for confidentiality and privacy breaches shall be capped and proportionate to bidder-attributable breach.	No Change, Please be guided by the RFP
1746	166-167		Penalty for blacklisting during contract period.	Exposure even where blacklisting may not relate to this engagement.	Modify: Applicable only where blacklisting relates directly to performance under this contract.	No Change, Please be guided by the RFP
1747	137		No reimbursement of travel, boarding, lodging or out-of-pocket expenses.	All implementation costs absorbed by bidder.	Clarify that customer-approved extraordinary expenses shall be reimbursable.	No Change, Please be guided by the RFP
1748	165-166		Delay in implementation may result in LD and additional penalties.	LD plus SLA penalties may create double recovery.	Clarify that LD and SLA penalties are mutually exclusive for the same event.	No Change, Please be guided by the RFP RFP Clause 13.2 - For the purpose of this RFP, the total penalties as per LD & SLA will be subject to a maximum of 10% of the overall contract value
1749	129+		Limited subcontracting permitted.	Restricts use of specialist service providers.	Request approval mechanism for subcontracting specialized services while retaining prime contractor responsibility.	No Change, Please be guided by the RFP No Subcontracting is allowed, Refer RFP
1750	162-163		All deliverables become Bank property.	May include bidder proprietary IP, templates and methodologies.	Clarify that pre-existing intellectual property, frameworks, tools and methodologies remain bidder property.	Details shall be shared with successful bidder
1751	137-140		Pricing fixed for contract duration.	Exposure to inflation, OEM cost increases and FX variation.	Request pass-through adjustment for OEM price increases, taxes and regulatory changes.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1752	160+		Arbitration / court proceedings largely controlled by Bank provisions.	Potential imbalance in dispute process.	Request neutral arbitration venue and equal participation in arbitrator selection.	No Change, Please be guided by the RFP
1753	165		Regulatory/statutory fines excluded from liability cap.	Unlimited financial exposure.	Modify: Regulatory penalties attributable to bidder shall be capped at annual contract value.	No Change, Please be guided by the RFP
1754	169-170		Separate Excel appendices	Appendix 1A, 1B, 1C, Appendix 2 and Appendix 3 are stated as separate Excel files.	Kindly provide the editable Excel versions of Appendix 1A, Appendix 1B, Appendix 1C, Appendix 2 Commercial BoM and Appendix 3 V2P Mapping, with protected cells and formulas identified, if any.	No Change, Please be guided by the RFP
1755	17-18		Masked BoM	Masked BoM must exactly replicate the Commercial BoM except price fields.	Please confirm whether bidder may add explanatory columns for OEM SKU, licence metric, deployment site, dependency and sizing assumptions while retaining all prescribed BoM rows unchanged.	The pricing shall be provided in the two separate sheets provided in the BOM/pricing template: Product License Cost: The bidder shall quote the applicable one-time perpetual license cost or initial subscription cost, as applicable, for the respective products/solutions. The relevant product/license details shall be provided in this sheet. ATS / Annual Subscription Cost: The bidder shall quote the applicable Annual Technical Support (ATS) / Annual Subscription Renewal Cost in the sheet provided for Y1 to Y5, post Go-Live. The bidder shall clearly identify the applicable licensing model (Perpetual/Subscription) for each product/solution and ensure that there is no duplication between the Product License Cost and ATS/Annual Subscription Cost. The BOM/pricing format remains unchanged.
1756	136		Right to descope	Bank may descope components before award while original scope remains evaluation basis.	Please clarify the method for adjusting dependent licences, infrastructure, implementation and support quantities when a solution component is descoped, and confirm that fixed/common platform costs will be retained where technically required.	Please refer addendum for revised clause.
1757	28,89-90		No additional cost / sizing risk	All omitted components and sizing shortfalls are to be supplied without additional cost.	Please confirm that no-cost augmentation applies only where the bidder/OEM sizing fails against the published volumetrics and agreed assumptions, and not where Bank inventory, growth, retention, integrations or scope exceed the RFP baseline.	The Bidder shall bear, at no additional cost to the Bank, all costs associated with correcting any omissions, errors, inadequacies, or sizing deficiencies in its proposal. Such corrections shall not result in any additional cost, delay, or reduction in the scope, performance, or service levels sought in the RFP
1758	159		Quantity variation	Bank may vary quantities by up to 25% at same unit prices.	Please confirm that the 25% variation will apply independently to measurable BoM line items and that SaaS/cloud consumption beyond contracted capacity will be ordered using quoted unit rates.	No Change, Please be guided by the RFP
1759	98		Extension pricing	Extension rates shall not exceed 120% of last-year AMC/ATS/FM rates.	Please confirm the treatment of SaaS subscription, cloud consumption, third-party feeds and OEM services during the optional extension where OEM list prices may change.	During any extension period, the applicable pricing shall be mutually agreed between the Bank and the Selected Bidder. The pricing shall not exceed 120% of the last year's AMC/ATS/Annual Subscription renewal charges/Facility Management rates quoted by the Selected Bidder for the respective solution/services
1760	29,35		Deception HA	Deployment matrix states Bank-side deception components are standalone, while deployment narrative refers to N+N Active-Active.	Please clarify the definitive HA requirement for deception agents, enforcers, decoys and honeypots at DC and DR, and whether management console HA is required.	Please refer addendum for revised clause
1761	258		SIEM capacity at DC & DR	SIEM is SaaS+Hybrid, yet volumetrics state 50,000 EPS scalable to 75,000 EPS at DC & DR.	Please confirm whether the EPS/TB capacity is aggregate enterprise ingestion, per site, or independently required at both DC and DR; also clarify whether Bank-side collectors/pipelines at each site must handle the full stated peak.	Please refer addendum for the revised clause
1762	259		UEBA capacity at DC & DR	UEBA is SaaS+Hybrid, yet volumetrics state capacity at DC & DR.	Please confirm whether UEBA EPS/data and endpoint-user capacities are aggregate enterprise quantities or required independently per DC and DR.	Please refer addendum for the revised clause
1763	31-35		N+N definition	Multiple hybrid components require N+N Active-Active at DC and DR.	Please define the minimum value of N and confirm whether N+N means two independent full-capacity nodes per site, with each node sized for 100% peak load.	No Change, Please be guided by the RFP
1764	91		Each node full peak load	Each node/environment must be individually provisioned for full peak load.	Please confirm whether this requirement applies to every node in an N+N cluster or to each site-level cluster, and whether OEM-supported load sharing with surviving-node capacity is acceptable.	No Change, Please be guided by the RFP
1765	89-92		Non-production separation	Production and non-production compute must be physically separate; VM non-production is minimum 10% of Production DC.	Please confirm whether a shared non-production compute cluster may host Dev, Test, UAT, Pre-Production and Training as logically isolated environments, and whether 10% is aggregate across those environments.	Please refer addendum for revised clause
1766	90-92		Network segmentation	Web, application and database tiers must be separated and east-west traffic routed through firewall/IPS.	Please confirm whether the Bank will provide existing firewall/IPS capacity and VLANs, or the bidder must supply dedicated security and network equipment for this segmentation.	No Change, Please be guided by the RFP
1767	94		Rack and power	Bank provides hosting space and power; bidder provides racks.	Please provide available rack dimensions, per-rack power limits, floor loading, PDU type, available RU at DC/DR and approved rack/PDU standards.	Details shall be shared with successful bidder
1768	67-69		Data residency	All Bank data, backups, logs, telemetry, prompts and metadata must reside within India.	Please confirm whether all primary, DR, backup, support-access and service-management components must be hosted and operated within India, and whether remote OEM support from outside India is prohibited or permitted through Bank-approved controlled access.	No Change, Please be guided by the RFP
1769	68		BYOK/CMEK	Cloud/SaaS solutions shall support BYOK and/or CMEK.	Please confirm whether BYOK/CMEK is mandatory for every SaaS solution or acceptable where the OEM provides dedicated tenant encryption using OEM-managed keys with compensating controls.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1770	68		Landing zones	Dedicated Dev, UAT and Production cloud landing zones are required.	Please confirm whether separate cloud tenants/subscriptions/accounts are mandatory for each environment, or logically segregated environments within the dedicated Bank tenant are acceptable.	Logical tenancy is acceptable, provided that the proposed bidder/OEM ensure clear separation and isolation of the Bank's data, security telemetry, logs, alerts, configurations, policies, analytics, investigation data and other Bank-related information from those of other tenants. The proposed environment for bank are protected against confidentiality and integrity risks and co-mingling of data and bidder/OEM implement adequate safeguards against combining of information, documents, records and assets.
1771	36-37		SIEM retention	Raw SIEM logs: 1 month; parsed/normalized/enriched/indexed/correlated logs: 60 months.	Please clarify the required storage tier for 60-month processed SIEM data, including the minimum period for online searchable retention, acceptable archive tier, retrieval SLA and expected query performance after restoration.	Please refer section7.2.4.3 Storage and other Requirement
1772	37		Other SaaS retention	Other SaaS solutions require at least 3 months primary storage.	Please confirm solution-wise data categories and whether 3 months means fully online/searchable retention for all telemetry, alerts, incidents, configurations and reports.	Please refer addendum for revised clause.
1773	36		Ingress and egress	All ingress, egress, API, inter-region, restoration, migration and exit charges are included.	Please provide estimated monthly data-transfer volumes and confirm that charges resulting from Bank-initiated bulk exports, forensic retrievals or scope growth beyond baseline will be handled through change control/unit rates.	Please refer section7.2.4.3 Storage and other Requirement
1774	68-69		Certifications	Cloud OEM shall have ISO 27001 certification and SOC 2 Type II report.	Please clarify whether the certification requirement applies to the solution OEM, underlying CSP, or both, and whether equivalent certifications/attestations are acceptable.	OEM of the propsoed solution providing the SaaS Solution
1775	68		AI model training	Bank data shall not be used for model training or retraining.	Please confirm whether aggregated, irreversibly anonymized service telemetry may be used for service improvement, or whether a complete contractual opt-out is mandatory.	No Change, Please be guided by the RFP
1776	34-36		Connectivity	Secure connectivity may use direct/private connectivity, VPN/IPSec and TLS 1.2+.	Please confirm whether Bank will provide internet/MPLS/direct-cloud connectivity and firewall changes, or bidder must include circuits, private links and recurring bandwidth charges.	The Bank is currently having MPLS and Internet services at its DC and DR locations. The Bank shall provide the required network connectivity, including MPLS/Internet connectivity, at the Bank's DC and DR locations. Necessary firewall/network changes within the Bank's existing infrastructure shall be coordinated by the Bank and shall be made in line with the Bank's policies.
1777	258		SIEM licence metric	50,000 EPS/2.06 TB per day, whichever is higher; average event size 500 bytes.	Please confirm whether licence entitlement must simultaneously cover both -have 50,000 EPS and 2.06 TB/day, and define the measurement window for sustainable EPS, peak/burst EPS and daily ingestion.	Please refer addendum for the revised clause
1778	258		SIEM growth tranches	Additional licences will be procured in 10,000 EPS/420 GB/day tranches.	Please confirm whether the unit rate should include matching storage, compute, collector capacity, support and cloud-transfer cost for the full remaining contract term.	The SIEM is being procured as a SaaS solution. Additional capacity shall be procured in 10,000 EPS / 420 GB/day tranches. The quoted rates shall include the required cloud infrastructure, storage, compute, connectivity and associated data-transfer costs as specified in the RFP.
1779	258		SOAR unrestricted use	SOAR has 5 concurrent users with no restriction on events, playbooks or actions.	Please confirm whether named users beyond five may access dashboards/approvals while only five users work concurrently, and whether all automation actions, integrations and playbooks must be unlimited.	No Change, Please be guided by the RFP
1780	258-259		XDR users	XDR required for 12,000 users scalable to 14,000.	Please confirm whether licensing is based on users, endpoints/devices, or both; provide expected counts by workstation, server, VDI and operating system.	Please refer addendum for revised clause.
1781	259	16.21.2 - Annexure 21, Volumetrics (NDR)	NDR throughput	NDR throughput requirement is 10 Gbps.	Please confirm whether 10 Gbps is per site, aggregate across DC/DR, full-duplex inspected throughput, or peak SPAN/TAP traffic; also provide number and speed of monitored links.	Please refer addendum for revised clause
1782	259		Deception scope	Coverage of 200 applications/networks/devices and 50 segments.	Please clarify whether 200 is the number of decoys, protected assets, credentials or monitored applications/devices, and provide segment/site distribution.	Please refer addendum for revised clause.
1783	260		AST licensing	SAST unlimited applications/scans/LOC with 30 users; DAST at least 25 applications.	Please define application, repository, branch and scan for licensing purposes, and provide language/framework, code-volume, API, mobile and CI/CD pipeline counts.	Details shall be shared with successful bidder
1784	260		CSPM quantity	CSPM specifies at least 20 VMs (VPCs).	Please clarify whether the required unit is 20 VMs, 20 VPCs/VNets, 20 cloud accounts/subscriptions, or a combination, and provide cloud-provider distribution.	No Change, Please be guided by the RFP
1785	260-261		CNAPP/CWPP overlap	CNAPP and CWPP each specify 20 VPCs/VNets and 100 VMs.	Please confirm whether the same 100 VMs and 20 VPCs/VNets are in scope for both solutions and whether a unified platform/SKU may satisfy both line items with separate compliance.	No Change, Please be guided by the RFP, bidder proposed solution should comply with the required volumetrics requirement, Further details shall be shared with the succesfull bidder
1786	261		CTEM unlimited metrics	CTEM requires unlimited findings, attack paths, exposures and remediation records.	Please confirm that commercial licensing may be based on the stated 12,000 users/4,000 IPs while the listed findings and relationships remain uncapped.	No Change, Please be guided by the RFP
1787	71,93-95		Feature/SKU changes	Committed functions must remain available despite OEM SKU/licensing changes.	Please confirm that this obligation is limited to capabilities included in the contracted edition/SKUs and does not require future separately developed products or modules not part of the awarded solution.	SLA
1788	89-93		Hardware quantities	Bidder must independently size all compute, storage, backup and network infrastructure.	Please provide the editable Appendix 1B and V2P template, existing rack/network standards, expected growth percentage, compression assumptions and workload profiles needed for equivalent bidder sizing.	Bidder can download the editable version from Bank's website mentioned in RFP
1789	89		Hardware vintage	Hardware must be latest production infrastructure not older than 2025.	Please clarify whether "not older than 2025" refers to model launch date, manufacturing date or delivery date, and confirm acceptance of current OEM-supported generation launched before 2025 but manufactured new.	Please refer addendum for revised clause.
1790	92,261-262		Backup and LTS duplication	Backup and LTS are required at both DC and DR.	Please confirm whether each site must independently retain a full copy of all backup/LTS data and whether cross-site replication counts as the second retained copy.	The bidder shall provide the backup and LTS necessary to meet the stated RFP requirements for both DC and DR. Each site (DC and DR) shall independently retain a complete copy of the applicable backup/LTS data.
1791	261-262		Backup sizing inputs	Retention is defined, but change rate and source-data volume are not.	Please provide solution-wise protected data volumes, daily change rate, expected compression/deduplication ratios, annual growth and required immutable/air-gapped copy specifications.	No Change, Please be guided by the RFP. Bidder to right size based on the proposed solution
1792	36-38,92-93		SaaS backup format	SaaS Bank-owned data must be transferred to Bank backup infrastructure and restorable.	Please specify required export frequency, format, API method, data consistency requirements and whether restoration must be back into the native SaaS platform or only retrievable/readable for audit and forensics.	The SIEM solution shall support real-time or near-real-time export/transfer of Bank data to the Bank's designated infrastructure.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1793	141		Spares	Critical hardware must be repaired/replaced or standby provided within four hours.	Please confirm whether onsite spares are mandatory for all hardware categories and specify the minimum spare inventory/location expectations.	No Change, Please be guided by the RFP
1794	75		Minimum resource count	Shift table specifies 12 L1, 5 L2 and 1 L3/PM, with additional L3 right-sized.	Please confirm whether these are minimum simultaneous shift positions or minimum named headcount, and whether weekly-off/leave relievers must be quoted as additional billable resources in the FM BoM.	No Change, Please be guided by the RFP The Resource requirement given in the RFP is minimum mandatory requirement that is to be deployed. It includes both DC & DR. Bidder can propose the manpower over and above if required.
1795	75		L3 shift coverage	Shift B and C L3/PM quantities are bidder to right-size.	Please confirm whether one L3/Operations PM in Shift A with on-call coverage is acceptable, or dedicated L3 presence is required in all three shifts.	No Change, Please be guided by the RFP
1796	72-74		Implementation team count	OEM and bidder implementation resources are full-time onsite but quantities are not specified.	Please confirm that implementation staffing may be proposed by the bidder/OEM through the resource plan, without a minimum resource count other than the dedicated onsite Project Manager.	No Change, Please be guided by the RFP The Resource requirement given in the RFP is minimum mandatory requirement that is to be deployed. It includes both DC & DR. Bidder can propose the manpower over and above if required.
1797	73-76		Resource locations	Resources may be deployed at SOC, DC, DR, branches or other Bank locations.	Please provide the primary work location, expected number of resources at each site and travel/on-call expectations for DC, DR and branches.	No Change, Please be guided by the RFP
1798	159		Payroll/subcontracting	All bidder personnel must be on bidder payroll; subcontracting is prohibited except OEM personnel.	Please confirm whether group-company employees, specialized staffing partners or CSP professional-services personnel are permitted with Bank approval.	All bidder personnel deployed for providing the Services shall be directly employed and on the payroll of the bidder, except OEM personnel expressly permitted. Bidder to submit the relevant ESIC/EPFO details of each deployed personnel for verification by the Bank.
1799	66		Training	15 Bank officials require certification; five sessions each of three training types per solution/OEM.	Please clarify whether the 5+5+5 sessions apply to each of the 14 solutions separately, and specify expected participant count per session, delivery mode and certification exam requirements.	
1800	54		Services licences not procured	Offsite services are subscriptions; solution licences are not to be procured.	Please confirm whether bidder may provide Bank portal/dashboard access essential for service delivery without transferring a software licence, and identify minimum user access required for each service.	No Change, Please be guided by the RFP
1801	32,55-58		Service scope volume	Frequencies are defined but asset/domain/user scope is not fully quantified.	Please provide service-wise volumetrics including domains, brands, mobile apps, executives, employees, phishing recipients, attack-surface assets and threat-hunting data sources.	details shall be shared with successful bidder
1802	147-148		Takedown SLA	Phishing takedown within 24 hours and brand abuse within 36 hours.	Please clarify that takedown SLA will be measured on best-effort coordination where third-party registrar/hosting/platform action is outside bidder control, and define exclusions/evidence requirements.	No Change, Please be guided by the RFP
1803	95		Existing SOC takeover	Existing solutions must be taken over from 01.05.2027 on as-is basis.	Please provide existing SOC tool inventory, OEM/support status, architecture, EPS, integrations, open incidents, manpower, SOPs, licence expiry dates and incumbent transition plan.	Details shall be shared with successful bidder, on need to know basis
1804	95		Existing SIEM parallel run	Existing SIEM must run for 12 months after new solution Go-Live.	Please confirm who will fund existing SIEM licences, OEM support and infrastructure during the 12-month parallel run, and whether these costs must be included in the bidder BoM.	The existing SIEM/SOC infrastructure and solution shall be operated and maintained by the bidder on an “as-is, where-is” basis during the parallel-run period, as required for compliance, at no additional cost to the Bank.
1805	78-79		Application use cases	Minimum 15 unique use cases per business application within six months.	Please confirm the number and list of business applications in scope for the 15-use-case requirement and whether the stated 200 applications are all included.	Details shall be shared with successful bidder
1806	143-144		Incident resolution	Critical/High resolution within 45 minutes, Medium 90 minutes, Low 150 minutes.	Please clarify whether resolution means permanent fix or service restoration/workaround, and whether OEM defect resolution is governed separately by OEM case SLA.	No Change, Please be guided by the RFP
1807	146-147		99.90% per component	Availability applies to each solution, infrastructure element and individual component.	Please confirm whether HA component failure without service impact counts as solution downtime, and define measurement points and approved exclusions.	Availability continues to be measured for each solution and any individual component. Failure of a redundant node/ component, even where the surviving node/component maintains service without functional or performance degradation, shall be tracked and penalized under Incident Response & Resolution Compliance (per the applicable Criticality Table timelines), rather than being excluded from measurement. Any failure of redundant node/ component shall be considered as a critical incident
1808	148-149		Utilization threshold	CPU/RAM/NIC/storage I/O above 75% for more than five minutes attracts penalties.	Please clarify whether short planned peaks, batch jobs, backup windows and vendor-recommended utilization ranges are excluded, and define the approved monitoring tool/sampling interval.	No Change, Please be guided by the RFP
1809	150		RPO/RTO penalty	RPO 15 minutes and RTO 60 minutes.	Please confirm whether RPO/RTO apply per solution and data class, and whether SaaS provider-native recovery is acceptable where customers cannot initiate regional failover.	No Change, Please be guided by the RFP. For SaaS solutions, if the SaaS provider itself manages backup, recovery, and failover between regions on the cloud provisoned, that arrangement is acceptable. The Bank does not necessarily need to have the ability to manually initiate regional failover on cloud. However, the SaaS solution must still meet the Bank's specified business continuity and disaster recovery requirements, including the applicable RPO/RTO
1810	155		OEM review penalty	INR 2,00,000 per affected solution per day for missed OEM review.	Please clarify the advance notice period, mutually agreed schedule and whether delays attributable to Bank rescheduling are excluded.	No Change, Please be guided by the RFP
1811	126,159		Multiple RFP award restriction	Successful bidder in another IT Security/Firewall RFP becomes ineligible here.	Please provide the exact referenced RFP numbers and clarify the stage at which cross-RFP ineligibility is determined, especially if commercial bids have already been opened.	Please refer addendum for revised clause.
1812	163		Make in India	PPP-MII Order and local-content certification apply.	Please confirm the applicable supplier class, minimum local-content threshold and whether local content is evaluated at overall bid, OEM solution or individual BoM line-item level.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1813	253-255		SBOM/CBOM	Detailed SBOM and CBOM fields are required for all tools/solutions.	Please confirm accepted formats such as SPDX/CycloneDX and clarify whether confidential component-level data may be submitted post-award under NDA, as indicated in Annexure 18.	The OEM shall maintain and periodically update the applicable SBOM, CBOM, AI-BOM and QBOM information in accordance with applicable CERT-In guidelines, regulatory requirements and prevailing industry standards. The relevant BOM information shall, as applicable, include identification of the component/asset, version, supplier/OEM, dependencies, relationships, vulnerabilities/security advisories, licensing information and relevant security attributes. Where a specific regulatory authority or applicable standard subsequently prescribes a particular schema, format or additional data elements, the OEM shall comply with the same during the contract period, subject to the applicable regulatory requirements. The bank will specify the BOM format/schema proposed, data elements captured, frequency of update, scope of coverage and mechanism inline with the requirement prescribed by regulator/statutory bodies.
1814	26,67		PQC readiness	All proposed solutions must be PQC ready.	Please define minimum accepted PQC-readiness criteria, required algorithms/standards, compliance evidence and expected implementation timeline.	The proposed solutions shall demonstrate a documented roadmap/capability for post-quantum cryptography readiness, including support for migration to applicable NIST-standardized PQC algorithms or approved industry standards as relevant to the solution. The bidder shall disclose current capability, dependencies and roadmap.
1815	26,70		SSL/TLS certificates	Bidder must provide required SSL/TLS certificates for contract period.	Please provide expected number, certificate types, public/private CA preference, wildcard/SAN requirements and whether Bank PKI-issued certificates are acceptable.	Details shall be shared with successful bidder
1816	Pg No-101	10.2 Eligibility Evaluation Criteria	Sl No-6-Eligibility Criteria/Clause	Bidder must have at least enrolled manpower (on bidder's payroll) of 100 experienced employees skilled in areas of Cyber security. Self-certification from the bidder	Request to kindly Amend- Bidder must have at least enrolled manpower (on bidder's payroll) of 100 experienced employees skilled in areas of Cyber security Self-certification from the bidder	No Change, Please be guided by the RFP
1817	Pg No-101	10.2 Eligibility Evaluation Criteria	Sl No-6-Eligibility Criteria/Clause	Bidder must have at least enrolled manpower (on bidder's payroll) of 100 experienced employees skilled in areas of Cyber security. Self-certification from the bidder	Request to kindly Amend- Bidder must have at least enrolled manpower (on bidder's payroll) of 100 experienced employees skilled in areas of Cyber security/IT /ITes. Self-certification from the bidder	No Change, Please be guided by the RFP
1818	Pg No-129	10.3 Technical Evaluation Criteria	Sl No-1-Bidder's Scoring Criteria	Bidder should have supplied, installed and maintained (or under maintenance) the below solutions in any one PSU/PSE/ Government Organizations / BFSI/Telecom provider in India 1. SOAR 2. UEBA 3. Extended Detection & response (XDR)/ Endpoint Detection & response (EDR) 4. Network Detection & response (NDR) 5. Threat Intelligence Platform 6. Vulnerability Assessment / Vulnerability Management 7. Identity Threat Detection & response (ITDR) 8. Decoy/Honeypot/Deception 9. Application security testing tool (DAST/SAST) 10. CSPM Point 1: Experience in 3 solutions – 8 Marks Point 2: Experience in 4 solutions –10 Marks Point 3: Experience in 5 solutions –12 Marks Point 4: Experience in more than 5 solutions– 15 Marks Max Marks – 15 Marks	Request to kindly Amend- Bidder should have supplied, installed and maintained (or under maintenance) the below solutions in any one PSU/PSE/ Government Organizations / BFSI/Telecom provider in India 1. SOAR 2. UEBA 3. Extended Detection & response (XDR)/ Endpoint Detection & response (EDR) 4. Network Detection & response (NDR) 5. Threat Intelligence Platform 6. Vulnerability Assessment / Vulnerability Management 7. Identity Threat Detection & response (ITDR) 8. Decoy/Honeypot/Deception 9. Application security testing tool (DAST/SAST) 10. CSPM Point 1: Experience in 3 solutions – 8 Marks Point 2: Experience in 4 solutions –10 Marks Point 3: Experience in 5 solutions –12 Marks Point 4: Experience in more than 5 solutions– 15 Marks Max Marks – 15 Marks	No Change, Please be guided by the RFP
1819	Pg No-129	10.3 Technical Evaluation Criteria	Sl No-1-Bidder's Scoring Criteria	Bidder should have supplied, installed and maintained (or under maintenance) the below solutions in any one PSU/PSE/ Government Organizations / BFSI/Telecom provider in India 1. SOAR 2. UEBA 3. Extended Detection & response (XDR)/ Endpoint Detection & response (EDR) 4. Network Detection & response (NDR) 5. Threat Intelligence Platform 6. Vulnerability Assessment / Vulnerability Management 7. Identity Threat Detection & response (ITDR) 8. Decoy/Honeypot/Deception 9. Application security testing tool (DAST/SAST) 10. CSPM Point 1: Experience in 3 solutions – 8 Marks Point 2: Experience in 4 solutions –10 Marks Point 3: Experience in 5 solutions –12 Marks Point 4: Experience in more than 5 solutions– 15 Marks Max Marks – 15 Marks	We understand that Experience of solution(s) can be shown in single /multiple Clients/work orders meeting the criteria(s)	Yes, your understanding is correct
1820	Pg No-98	9-Project Timeline	9-Project Timeline	Overall Implementation period shall be 5 Months (Start Date is T0) for all solution & services The bidder shall submit a comprehensive Project Plan, within 7 days of T0 covering each proposed product/solution & Services, detailing all project phases, milestones, tasks, sub-tasks, activities, timelines, dependencies. The bidder shall submit the detailed Project Plan along with the proposal (mandatory) and subsequently within seven (7) days from T0 for the Bank's review and approval. Any Liquidated Damages (LD) for delays in project execution shall be calculated based on the bank's approved Project Plan.	Request to kindly Amend for timely completion of Project- Overall Implementation period shall be 5 10 Months (Start Date is T0) for all solution & services The bidder shall submit a comprehensive Project Plan, within 7 days of T0 covering each proposed product/solution & Services, detailing all project phases, milestones, tasks, sub-tasks, activities, timelines, dependencies. The bidder shall submit the detailed Project Plan along with the proposal (mandatory) and subsequently within seven (7) days from T0 for the Bank's review and approval. Any Liquidated Damages (LD) for delays in project execution shall be calculated based on the bank's approved Project Plan.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1821	Pg-163	14.14 Make in India	14.14 Make in India	The local supplier at the time of submission of bid shall be required to provide a certificate as per Annexure 7 from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content. The Bank shall follow all the guidelines/ notifications for public procurement.	Request to Amend- The local supplier at the time of submission of bid shall be required to provide a certificate as per Annexure 7 from the Charter Accountant or statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content. The Bank shall follow all the guidelines/ notifications for public procurement.	No Change, Please be guided by the RFP
1822	Pg-137	12 -Payment Terms	12.1 Product (Software) Cost	Product License Cost- On successful delivery of the licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware. The Bidder is required to submit the required to submit the following:--15% • Delivery proof • OOTB Installation Proof • Invoice of the Product On successful UAT Signoff of the respective product-20% On successful Go-live of the respective product-30% Product Implementation Cost- On Successful installation of OOTB product on the sourced hardware and handing over the environment with OOTB product to Bank -20% On successful UAT Signoff of the respective product-50% On successful Go-live of the respective product-20% Subscription Cost (One time license (Cost) On successful delivery of the Licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware.- 50% The Bidder is required to submit the required to submit the following • Delivery proof • OOTB Installation Proof	Request to Amend the Payment Terms for Positive Cashflow- Product License Cost- On successful delivery of the licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware. The Bidder is required to submit the required to submit the following:--15% 80% on Pro Rata • Delivery proof • OOTB Installation Proof • Invoice of the Product On successful UAT Signoff of the respective product-20% 10% On successful Go-live of the respective product-30% 10% Product Implementation Cost- On Successful installation of OOTB product on the sourced hardware and handing over the environment with OOTB product to Bank -20% 80% on Pro Rata On successful UAT Signoff of the respective product-50% 10% On successful Go-live of the respective product-20% 10% Subscription Cost (One time license (Cost) On successful delivery of the Licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware.- 50% 80% on Pro Rata The Bidder is required to submit the required to submit the following • Delivery proof • OOTB Installation Proof	No Change, Please be guided by the RFP
1823	Pg- 138	Section 12-Payment Terms	12.3 Hardware Cost	Hardware Cost- Appliance Cost-On successful Delivery of the Appliance which would be considered delivered once the solution (with OOTB features) is made available for view and review of the bank-50% The Bidder is required to submit the required to submit the following: • Delivery proof • OOTB Installation Proof • Invoice of the Product On successful UAT Signoff of the respective product-20% On successful Go-live of the respective product-30% Hardware Cost (Other than Appliances) Delivery of hardware and submission of invoice with Proof of Delivery and other documents of the hardware supplied. Bank may at its discretion verify the details before releasing the payment-70% On successful installation of proposed solutions on the hardware - 50% of the sought product/solutions-15% On successful installation of remaining proposed solution on the hardware – remaining 50% of the sought product/solutions-15%	Request to Amend the Payment Terms for Positive Cashflow- Hardware Cost- Appliance Cost-On successful Delivery of the Appliance which would be considered delivered once the solution (with OOTB features) is made available for view and review of the bank-50% 80% on Pro Rata The Bidder is required to submit the required to submit the following: • Delivery proof • OOTB Installation Proof • Invoice of the Product On successful UAT Signoff of the respective product-20% 10% On successful Go-live of the respective product-30% 10% Hardware Cost (Other than Appliances) Delivery of hardware and submission of invoice with Proof of Delivery and other documents of the hardware supplied. Bank may at its discretion verify the details before releasing the payment-70% 85% on Pro Rata On successful installation of proposed solutions on the hardware - 50% of the sought product/solutions-15% 10% On successful installation of remaining proposed solution on the hardware – remaining 50% of the sought product/solutions-15% 5%	No Change, Please be guided by the RFP
1824	Pg- 25	6.20 Fixed Price	6.20 Fixed Price	The prices quoted in the tender response will be fixed for the period of the contract. The price should be exclusive of all taxes and levies which will be paid by the Bank on actua	Request to Amend- The prices quoted in the tender response will be fixed for the period of the contract till Go live Period. The price should be exclusive of all taxes and levies which will be paid by the Bank on actua	No Change, Please be guided by the RFP
1825	Pg- 165	14.19 Liquidated Damages		The Bank will consider the inability of the bidder to deliver or install the equipment & provide the services required within the specified time limit as a breach of contract and would entail the payment of Liquidated Damages on the part of the bidder. The liquidated damages represent an estimate of the loss or damage that the Bank may have suffered due to delay in performance of the obligations (relating to delivery, installation, operationalization, implementation, training, acceptance, warranty, maintenance etc. of the proposed solution/services) by the bidder. Installation will be treated as incomplete in one / all the following situations: 1. Non-delivery of any component or other services mentioned in the order 2. Non-delivery of supporting documentation 3. Delivery / availability, but no installation of the components and software 4. No integration/ Incomplete Integration 5. Non-Completion of Transition within suggested timeline 6. System operational, but not as per SLA, Timelines and scope of the RFP If the bidder fails to deliver any or all of the products, systems and services solutions within the time period(s) specified in the Delivery Schedule or installation, the Bank shall, without	Request to Amend- The Bank will consider the inability of the bidder to deliver or install the equipment & provide the services required within the specified time limit as a breach of contract and would entail the payment of Liquidated Damages on the part of the bidder. The liquidated damages represent an estimate of the loss or damage that the Bank may have suffered due to delay in performance of the obligations (relating to delivery, installation, operationalization, implementation, training, acceptance, warranty, maintenance etc. of the proposed solution/services) by the bidder. Installation will be treated as incomplete in one / all the following situations: 1. Non-delivery of any component or other services mentioned in the order 2. Non-delivery of supporting documentation 3. Delivery / availability, but no installation of the components and software 4. No integration/ Incomplete Integration 5. Non-Completion of Transition within suggested timeline 6. System operational, but not as per SLA, Timelines and scope of the RFP If the bidder fails to deliver any or all of the products, systems and services solutions within the time period(s) specified in the Delivery Schedule or installation, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 0.5 percent per week on prorata or part thereof of Contract Price subject to maximum deduction	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1826	Pg- 159	14 TERMS AND CONDITIONS	14.1 Assignment & Subcontracting	1. The selected bidder shall not subcontract/JV/Consortium or permit anyone to perform any of the work, service or other performance required under the contract (excluding Proposed OEM personnels). All bidder's personnel proposed for the bank shall be on bidder' Payroll. Bank will seek relevant documentation from the bidder to validate the same.	Request to Amend - 1. The selected bidder shall not subcontract/JV/Consortium or permit anyone to perform any of the work, service or other performance required under the contract (excluding Proposed OEM personnels). All bidder's personnel proposed for the bank shall be on bidder Payroll. Bank will seek relevant documentation from the bidder to validate the same.	No Change, Please be guided by the RFP
1827	Pg-157	13.2 Penalties	13.2 Penalties	For the purpose of this RFP, the total penalties as per LD & SLA will be subject to a maximum of 10% of the overall contract value. Liquidated Damages Supply & Delivery Please refer to section 14.19 for LD on Supply & Delivery Installation & Implementation Delay in delivery, installation, configuration, integration, testing, commissioning, migration, implementation, Go-Live, or any project milestone approved by the Bank., the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 1% per week or part thereof of the respective Product Cost subject to maximum deduction of 10% of the total contract value, until actual delivery and implementation as per related clauses mentioned in RFP. * Product Cost = Product License/Subscription Cost + Implementation + Configuration + Integration + Migration + Commissioning Cost. If the LD due to Implementation of the respective product cost/existing product cost reaches 25% of the implementation cost of the respective product/services, the bidder is required to replace the product/services. Once the maximum deduction is reached, the Bank may consider termination of the	Request to Amend- For the purpose of this RFP, the total penalties as per LD & SLA will be subject to a maximum of 10% of the overall contract value. Liquidated Damages Supply & Delivery Please refer to section 14.19 for LD on Supply & Delivery Installation & Implementation Delay in delivery, installation, configuration, integration, testing, commissioning, migration, implementation, Go-Live, or any project milestone approved by the Bank., the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 1% per week or part thereof of the respective Product Cost subject to maximum deduction of 10% of the total contract value, until actual delivery and implementation as per related clauses mentioned in RFP. * Product Cost = Product License/Subscription Cost + Implementation + Configuration + Integration + Migration + Commissioning Cost. If the LD due to Implementation of the respective product cost/existing product cost reaches 25% of the implementation cost of the respective product/services, the bidder is required to replace the product/services. Once the maximum deduction is reached, the Bank may consider termination of the Contract at its discretion. issue a performance warning or initiate corrective actions	No Change, Please be guided by the RFP
1828	Pg-17	Instruction to Bidder	6.4.1, Part A	The bidder must submit a complete Technical cum Eligibility Proposal and a masked BoM.	Kindly confirm whether a bidder may propose multiple OEMs for different solution components under a single integrated response, subject to submission of separate OEM authorization and compliance documents.	No Change, Please be guided by the RFP
1829	Pg-19	Technical Normalization	6.6	The Bank may normalize sizing, capacity, licensing, deployment architecture, and performance requirements and may load the evaluated cost of additional components.	Kindly request the Bank to publish the detailed normalization methodology, including the baseline assumptions for EPS, storage, users, endpoints, cloud resources, HA, DR, retention, and licensing, to ensure transparent and comparable bidding.	No Change, Please be guided by the RFP
1830	Pg-26–28	Scope of Work	7.1	The bidder/OEM must provide customization, enhancement, parser development, connector creation, workflow automation, dashboard customization, reporting customization, and alert tuning without additional cost throughout the contract period.	Kindly define the expected minimum number of parsers, connectors, playbooks, dashboards, reports, and use cases to be developed annually. Alternatively, kindly clarify whether these activities will be governed by a mutually agreed annual effort or change-request limit.	No Change, Please be guided by the RFP
1831	Pg-26–28	Scope of Work	7.1	The bidder is responsible for all components required for successful implementation, operation, scalability, and completeness of the solution.	Kindly clarify whether the Bank will provide the required network connectivity, firewall rules, DNS, IP addresses, rack space, power, cooling, virtualization platform, operating system, database, and storage, or whether all such infrastructure must be included in the bidder's scope.	The hosting space and power arrangements shall be provided by the Bank at the DC and DR locations. The Bank currently has MPLS and Internet services at its DC and DR locations and shall provide the required network connectivity, including MPLS/Internet connectivity, at the Bank's DC and DR locations. Necessary firewall/network changes within the Bank's existing infrastructure shall be coordinated by the Bank and shall be carried out in line with the Bank's policies. Any other components, infrastructure, licenses or services required for the proposed solution shall be factored in by the Bidder within its scope and commercial proposal
1832	Pg-27	Scope of Work	7.1, Key Implementation Responsibilities	Implementation of each solution, including design, installation, integration, testing, UAT, and Go-Live, shall be performed by the respective OEM.	Kindly clarify whether the bidder may use OEM-authorized implementation partners or certified system integrators where the OEM does not directly provide local implementation resources.	No Change, Please be guided by the RFP
1833	Pg-29–35	Deployment Model	7.2 and 7.2.4	Multiple solutions require Cloud/SaaS plus hybrid deployment, with N+N Active-Active components at DC and DR.	Kindly confirm whether the Bank has approved any specific CSPs. If not, may the bidder propose an RBI-/CERT-In-compliant CSP based on data residency, availability, security, and regulatory requirements?	No Change, Please be guided by the RFP
1834	Pg-29–35	Deployment Model	7.2.1 and 7.2.4	Management consoles are required at both Primary and Secondary sites for several solutions.	Kindly clarify whether a single logical cloud management console with resilient access from both DC and DR will be accepted, where the OEM architecture does not support separate independent management consoles at both locations.	No Change, Please be guided by the RFP
1835	Pg-31–33	Deployment Model	7.2.1, 7.2.3 and 7.2.4	Partial HA of critical Bank-hosted components is not accepted and N+N Active-Active is mandated.	Kindly clarify whether OEM-native clustering, distributed architecture, load balancing, or cloud-native HA mechanisms that provide equivalent or better availability will be accepted in lieu of physical N+N Active-Active deployment.	No Change, Please be guided by the RFP
1836	Pg-36	Connectivity and Data Flow	7.2.4.2	Data transmission to cloud platforms shall use controlled connectivity mechanisms including private/direct connectivity, VPN/IPSec, and TLS 1.2+.	Kindly confirm whether the Bank will provide the required private connectivity or VPN termination. If bidder-provided connectivity is required, kindly provide expected bandwidth, latency, redundancy, and responsibility demarcation.	The hosting space and power arrangements shall be provided by the Bank at the DC and DR locations. The Bank currently has MPLS and Internet services at its DC and DR locations and shall provide the required network connectivity, including MPLS/Internet connectivity, at the Bank's DC and DR locations. Necessary firewall/network changes within the Bank's existing infrastructure shall be coordinated by the Bank and shall be carried out in line with the Bank's policies. Any other components, infrastructure, licenses or services required for the proposed solution shall be factored in by the Bidder within its scope and commercial proposal
1837	Pg-36–39	Storage and Retention	7.2.4.3	Cloud solutions must support long-term archival on the Bank's designated infrastructure, with no additional cost for data ingress, egress, retrieval, restoration, or migration.	Kindly provide details of the Bank's designated archival and backup infrastructure, supported protocols, available bandwidth, storage technology, and preferred data-transfer mechanism for accurate sizing and costing.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1838	Pg-36–39	Storage and Retention	7.2.4.3	The bidder must provide storage sizing for the complete contract period, including growth, indexing, compression, replication, backup, and archival overheads.	Kindly confirm the assumed annual growth rate and whether the Bank will provide final historical data volumes, source-wise log volumes, average event size, peak EPS, and retention requirements before solution sizing is finalized.	No Change, Please be guided by the RFP
1839	Pg-37	SIEM	7.2.4.3, SIEM Storage	Raw SIEM logs must be retained for one month and parsed, normalized, enriched, indexed, and correlated logs for 60 months.	Kindly clarify whether the 60-month retention requirement applies to all normalized and indexed data or only security-relevant data selected by the Bank. Kindly also confirm whether archived data may be stored in a searchable or cold-storage format.	Please refer addendum for revised clause
1840	Pg-37	SIEM	7.2.4.3, SIEM Backup	Raw and processed SIEM logs, configurations, policies, rules, metadata, and Bank-owned data must be backed up/transferred to the Bank's DC and DR infrastructure.	Kindly clarify whether the Bank will provide the required backup storage capacity and backup platform licenses, or whether the bidder must include these components in the BoM.	The Bidder shall provision the required backup storage, infrastructure and associated components to meet the backup and retention requirements specified in the RFP
1841	Pg-39–40	SIEM	7.3.1.1	SIEM must integrate with the Bank's entire IT ecosystem, including current, future, legacy, on-premises, cloud, and hybrid infrastructure.	Kindly provide the current and anticipated list of log sources, applications, databases, network devices, security tools, cloud platforms, APIs, and estimated source count to enable accurate licensing, sizing, and implementation planning.	Details shall be shared with successful bidder
1842	Pg-40	SIEM	7.3.1.1, Clause 7	All SIEM components must operate in the prescribed HA architecture at DC, DR, CSP primary, and CSP secondary sites.	Kindly clarify whether the requirement refers to logical availability of the complete SIEM service or requires duplicate licensing and full-capacity infrastructure at every location.	The applicable SIEM components shall be deployed in N+N Active-Active HA at DC and DR, while Cloud/SaaS HA shall align with the SLA, RTO and RPO requirements; the Management Console shall be deployed at both Primary and Secondary sites.
1843	Pg-40–41	SIEM	7.3.1.1, Clauses 8 and 7.3.1.2	The bidder must disclose input EPS, processed EPS, filtered/suppressed events, final EPS, and the methodology for measuring EPS.	Kindly confirm whether EPS will be measured using the OEM's native metering mechanism, an independent monitoring tool, or a Bank-approved measurement methodology.	No Change, Please be guided by the RFP 7.3.1.2 SIEM Data Ingestion and EPS Measurement
1844	Pg-41	SIEM	7.3.1.2	SIEM EPS is defined as unique records actually delivered to and ingested by the SIEM for processing.	Kindly clarify how the Bank will treat multi-line events, duplicate events received from multiple collectors, batched events, compressed events, flow records, and events generated by agents or brokers.	The Bidder shall design the solution to ensure that duplicate events are not generated or counted towards SIEM EPS.
1845	Pg-41	SIEM	7.3.1.2	XDR/native telemetry must not be double-counted as SIEM EPS where it is not separately ingested by SIEM.	Kindly confirm that where a unified OEM platform uses a common data lake and a single ingestion pipeline, the bidder may provide an auditable logical allocation of data between SIEM and XDR instead of duplicate licensing.	Bidder to design the solution
1846	Pg-41–42	SIEM	7.3.1.1 and 7.3.1.3	SIEM must support AI-assisted investigation, threat hunting, root-cause analysis, query generation, and recommended response actions.	Kindly clarify the minimum expected AI/ML capabilities, supported languages, data-processing location, data privacy controls, model-training approach, explainability requirements, and whether use of external generative AI services is permitted.	No Change, Please be guided by the RFP
1847	Pg-42	SIEM	7.3.1.3	The bidder must create and maintain customized parsers for unknown/customized log sources without additional cost.	Kindly clarify the expected turnaround time for development and deployment of a new parser and the required format and minimum information to be provided by the Bank for such development.	Details shall be shared with successful bidder
1848	Pg-42	SOAR	7.3.2.2	SOAR shall integrate with SIEM, XDR, NDR, UEBA, TIP, ITSM, IAM/PAM, network, endpoint, cloud, and other solutions.	Kindly provide the list of existing products and versions for which integration is required. Where native connectors are unavailable, kindly confirm whether REST API, webhook, script, or custom connector-based integration will be accepted.	Details shall be shared with successful bidder
1849	Pg-42	SOAR	7.3.2.2	Development, customization, testing, tuning, and maintenance of organization-specific playbooks are included without additional cost.	Kindly specify the minimum number of SOAR playbooks expected during implementation and annually during operations.	No Change, Please be guided by the RFP
1850	Pg-43	UEBA	7.3.3	UEBA must integrate the entire IT infrastructure and support extremely high IOPS at collection, correlation, and alerting layers.	Kindly provide the estimated number of users, entities, applications, endpoints, data sources, authentication events, and peak IOPS to enable accurate sizing and performance validation.	Details shall be shared with successful bidder
1851	Pg-43	UEBA	7.3.3	UEBA is required to provide complete replay of the attack kill-chain lifecycle from reconnaissance to evidence destruction.	Kindly clarify whether this requirement may be met through integrated SIEM, XDR, NDR, TIP, and forensic capabilities rather than through native UEBA functionality alone.	No Change, Please be guided by the RFP
1852	Pg-44–45	XDR/NDR	7.3.4 and 7.3.5	XDR and NDR must provide continuous visibility, detection, investigation, threat hunting, forensics, and response.	Kindly clarify whether the Bank will provide endpoint agents, network TAP/SPAN feeds, packet brokers, cloud telemetry, and required endpoint/network access, or whether these must be included in the bidder's scope.	Please refer addendum for the revised clause
1853	Pg-45	Decoy/Honeypot	7.3.6	The proposed deception solution must cover at least 200 applications, networks, and devices with 50 segments across DC and DR.	Kindly provide the expected distribution of the 200 decoys across applications, servers, network devices, endpoints, databases, and segments. Also clarify whether licenses must be sized for 200 simultaneous decoys.	Please refer addendum for the revised clause
1854	Pg-45–46	Threat Intelligence Platform	7.3.7	The TIP must aggregate, normalize, enrich, score, distribute, and expire indicators from multiple intelligence sources.	Kindly clarify the minimum number and type of threat-intelligence feeds expected, including commercial, open-source, dark-web, malware, vulnerability, brand-protection, and sector-specific feeds.	Details shall be shared with successful bidder
1855	Pg-47	VA/VM	7.3.8	VA must support authenticated and unauthenticated assessments across infrastructure, applications, identities, cloud, endpoints, and authentication environments.	Kindly provide the estimated number of IPs, domains, applications, cloud assets, credentials, scanning windows, and frequency of assessments required for sizing and licensing.	No Change, Please be guided by the RFP
1856	Pg-47–48	ITDR	7.3.9	ITDR must integrate with Active Directory, LDAP, IAM, PAM, SSO, cloud identity providers, and other identity repositories.	Kindly provide the list of identity sources, versions, number of domains, users, service accounts, privileged identities, and expected authentication-event volume.	Please refer addendum for revised clause.
1857	Pg- 48–49	AST	7.3.10	AST shall cover SAST, DAST, API, mobile security, SCA, container scanning, and CI/CD integration.	Kindly provide the number of applications, APIs, mobile applications, repositories, container registries, developers, pipelines, and expected scans per year for accurate sizing.	The bidder shall size its proposal based on the RFP volumetrics
1858	Pg-49–53	CSPM/CNAPP/CWPP/CTEM	7.3.11–7.3.14	Several cloud-security solutions are required across multi-cloud, hybrid-cloud, on-premises, containers, Kubernetes, identities, and workloads.	Kindly provide the current and planned cloud service providers, accounts/subscriptions/projects, VPCs/VNETs, regions, VM counts, containers, Kubernetes clusters, workloads, identities, and cloud-native services in scope.	Details shall be shared with successful bidder
1859	Pg-54–58	Offsite Services	7.4	Managed services include BAS, automated red teaming, ASM, phishing simulation, anti-phishing, dark-web monitoring, TIP feeds, threat hunting, and brand protection.	Kindly confirm the expected number of domains, IP ranges, applications, brands, employees, phishing campaigns, dark-web keywords, social-media assets, and threat-hunting hours included in the scope.	No Change, Please be guided by the RFP
1860	Pg-54–58	Offsite Services	7.4	Several offsite services require continuous or 24×7 monitoring and periodic reporting.	Kindly clarify whether the services must be delivered from a CERT-In-empanelled facility, whether offshore resources are permitted, and whether all service data must remain within India.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1861	Pg-58–59	Bidder/OEM Responsibilities	7.5 and 7.6	Bidder and OEM are jointly responsible for end-to-end implementation, integration, support, documentation, training, and operations.	Kindly clarify the responsibility matrix between the system integrator, respective OEMs, CSP, Bank, and third-party service providers.	No Change, Please be guided by the RFP
1862	Pg-68–69	Non-Functional Requirements	7.8	The RFP requires enterprise-grade, production-grade, OEM-supported, GA releases throughout the contract period.	Kindly confirm whether a solution currently in a controlled release, limited availability release, or OEM-supported long-term support release will be accepted where it is recommended by the OEM for enterprise deployment.	No Change, Please be guided by the RFP
1863	Pg-69–70	Delivery and Commissioning	7.9	The solution must be delivered, installed, commissioned, tested, and accepted in accordance with the RFP.	Kindly provide the expected implementation timeline and milestone dates for each solution, including dependencies on Bank-provided infrastructure, connectivity, access, credentials, and third-party integrations.	No Change, Please be guided by the RFP
1864	Pg-71	Data Privacy	7.1	The RFP requires compliance with applicable Indian data-protection and privacy laws.	Kindly clarify the required data residency location for cloud-hosted security telemetry, backups, metadata, support logs, and diagnostic data.	No Change, Please be guided by the RFP
1865	Pg-72	Warranty, ATS and AMC	7.11	Comprehensive ATS/AMC support is required for all proposed solutions, components, hardware, software, and services.	Kindly clarify whether the ATS/AMC period commences from the date of Go-Live, final acceptance, or delivery of the respective component.	No Change, Please be guided by the RFP
1866	Pg-72–75	Resource Requirement	7.12	Onsite L1, L2, and L3 resources and offsite OEM SMEs are required.	Kindly provide the minimum number, role, shift pattern, skill level, certification, location, and working hours for each onsite and offsite resource category.	No Change, Please be guided by the RFP
1867	Pg-75	Resource Deployment	7.12.4	Minimum resource count deployment is specified in the RFP.	Kindly confirm whether the minimum resource count is to be maintained per shift, per location, or as the total headcount across all shifts and locations.	No Change, Please be guided by the RFP The Resource requirement given in the RFP is minimum mandatory requirement that is to be deployed. It includes both DC & DR. Bidder can propose the manpower over and above if required.
1868	Pg-77–83	Facilities Management	7.13	The bidder is responsible for comprehensive maintenance, monitoring, backup, recovery, troubleshooting, upgrades, integration, and related activities without additional charges.	Kindly clarify the boundary between facilities management of Bank-provided infrastructure and maintenance of bidder/OEM-provided infrastructure, including replacement responsibility and spares.	No Change, Please be guided by the RFP
1869	Pg-80	Facilities Management	7.13, Clause 31	All critical/showstopper feature requests declared by the Bank must be implemented within one week.	Kindly request the Bank to define "critical" and "showstopper" feature requests and confirm that OEM product-roadmap limitations, major version upgrades, and changes requiring formal development will be handled through an agreed change-management process.	"Critical" and "showstopper" shall be determined by the Bank based on security, regulatory, operational or business impact. The bidder shall provide immediate workaround/remediation where a product limitation prevents permanent implementation within the stipulated time. Product roadmap limitations shall not automatically excuse a contractual requirement.
1870	Pg-80–81	Facilities Management	7.13, Clauses 34–36	Proposed solutions must be PQC-ready, support IPv6, and provide data/logs to CERT-In, NCIIPC, CSITE, and other regulators.	Kindly clarify the expected technical interpretation of "PQC-ready," the applicable cryptographic standards, the meaning of "CSITE," and the prescribed data format/API for regulatory sharing.	No Change, Please be guided by the RFP, CSITE here refer to audit by RBI
1871	Pg-80–81	Facilities Management	7.13, Clause 44	If performance is not satisfactory, the bidder/OEM must upgrade hardware, software, or applications at no additional cost.	Kindly clarify the objective acceptance and performance criteria that will be used to determine unsatisfactory performance and the process for jointly validating any required upgrade.	No Change, Please be guided by the RFP
1872	Pg-81	Facilities Management	7.13, Clause 46	Additional features or capabilities available through license activation must be provided without extra cost.	Kindly clarify whether this requirement applies only to features included in the quoted license entitlement or also to separately chargeable OEM modules and subscriptions.	No Change, Please be guided by the RFP
1873	Pg-83–84	DR Drill/System Recovery	7.14 and 7.17	Quarterly or periodic DR drills are required, with full coordination among the bidder, OEM, Bank, application teams, and other vendors.	Kindly provide the required RTO and RPO for each solution and clarify whether DR drill execution outside the planned quarterly schedule will be treated as an included activity or a change request.	No Change, Please be guided by the RFP
1874	Pg-84–87	NextGEN SOC Operations	7.15	The bidder must conduct continuous operations, develop custom plug-ins/parsers/connectors, perform gap analysis, create use cases, support drills, and provide reports without additional cost.	Kindly specify the expected number of log sources, custom integrations, use cases, dashboards, reports, automation workflows, and threat-hunting exercises to be delivered during the implementation and each contract year.	No Change, Please be guided by the RFP
1875	Pg-85	NextGEN SOC Operations	7.15, Clause 19	The Bank's ticketing tool must be used for all operational activities.	Kindly provide the name, version, deployment model, API capability, authentication method, and integration requirements of the Bank's ticketing tool.	ITSM - Manage Engine
1876	Pg-85–86	NextGEN SOC Operations	7.15, Clause 23	Comprehensive AMC/ATS includes all versions, patches, fixes, updates, security alerts, documentation, and 24×7 support.	Kindly clarify whether major-version upgrades involving migration, re-architecture, additional infrastructure, or separate OEM professional services are included in the quoted AMC/ATS cost.	No Change, Please be guided by the RFP
1877	Pg-87	Infrastructure Management	7.15, Clause 24	Bidder must provide monitoring, backup, restoration, application, database, storage, and solution management.	Kindly clarify the Bank's responsibility for providing administrative access to operating systems, databases, storage, virtualization, network, cloud, backup, and security infrastructure.	The Bank shall provide necessary access, connectivity and coordination for Bank-managed infrastructure, subject to the Bank's applicable security controls and approval processes. The Bidder shall remain responsible for monitoring, management, backup, restoration and other activities within its scope as specified in the RFP.
1878	Pg-87–88	OEM Services	7.16	OEM architecture assessment and performance review are required from Year 2 onwards at specified frequencies.	Kindly confirm whether the assessment must be conducted by OEM personnel physically onsite or whether remote assessment by certified OEM experts, followed by an onsite review where required, will be accepted.	No Change, Please be guided by the RFP
1879	Pg-88	Incident Handling	7.16	Critical incident resolutions must be reviewed and formally certified by the respective OEM.	Kindly clarify the expected turnaround time for OEM certification and whether an OEM technical-support case closure report or official RCA will satisfy this requirement.	No Change, Please be guided by the RFP
1880	Pg-89–93	IT Infrastructure	7.18	Bidder must provide or manage compute, storage, backup, networking, security equipment, software, and associated infrastructure.	Kindly provide the current infrastructure inventory, available capacity, virtualization platform, operating-system standards, storage platform, backup solution, network topology, and data-centre constraints for final sizing.	details shall be shared with successful bidder
1881	Pg-98	Contract Period	Section 8	Contract period and extension provisions are referenced but not fully detailed in the available section.	Kindly specify the exact contract duration and whether the Bank may extend the contract annually at the same unit rates, terms, and SLA conditions.	No Change, Please be guided by the RFP
1882	Pg-98	Project Timelines	Section 9	Project timelines are prescribed in the RFP.	Kindly provide a detailed solution-wise implementation schedule and clarify whether timelines will be extended where dependencies such as access, infrastructure, data, connectivity, or third-party approvals are delayed by the Bank.	No Change, Please be guided by the RFP
1883	Pg-104–105	Eligibility Criteria	Section 10.2	The bidder must have successfully supplied, installed, and maintained a SIEM solution of at least 20,000 EPS or 0.86 TB/day in one PSU/PSE/government/BFSI/telecom organization.	Kindly confirm whether the SIEM capacity may be demonstrated through a combination of EPS and daily ingestion capacity across the same project, provided that the implementation satisfies either threshold.	Please refer addendum for revised clause.
1884	Pg-106–107	Eligibility Criteria	Section 10.2	Client-issued documents must establish client name, project scope, solution name, OEM, status, and contract period.	Kindly confirm whether confidential client documents may be submitted with commercially sensitive information redacted, provided the required eligibility details remain verifiable.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1885	Pg-111–113	Eligibility Criteria	Section 10.2	The proposed OEM SIEM solution must have been implemented at 30,000 EPS or 1.2 TB/day in at least one BFSI organization and implemented on cloud in India.	Kindly clarify whether the BFSI client may be a global banking/financial-services entity with implementation hosted in India, and whether a cloud deployment under a managed private-cloud model will qualify as an implementation on cloud.	Please refer addendum for revised clause.
1886	Pg-113	Eligibility Criteria	Section 10.2	The proposed OEM solution must have been implemented in at least one BFSI organization for SOAR, UEBA, XDR, NDR, and TIP.	Kindly clarify whether each proposed OEM must independently satisfy the BFSI implementation requirement for all applicable solutions or whether the requirement may be met collectively by the bidder's proposed OEM ecosystem.	No Change, Please be guided by the RFP
1887	Pg-129–135	Technical Evaluation	Section 10.3	Technical evaluation includes solution compliance, experience, resources, architecture, and other criteria.	Kindly request the Bank to publish the detailed technical scoring matrix, minimum qualifying technical score, scoring for partial compliance, and treatment of "complied with deviation" responses.	No Change, Please be guided by the RFP
1888	Pg-135	Commercial Evaluation	Section 10.4	Commercial evaluation is based on the prescribed BoM and TCO.	Kindly clarify whether the evaluated commercial price will include optional quantities, future scalability tranches, cloud egress, data transfer, regulatory audits, travel, onsite OEM visits, and all potential extension periods.	The Bidder shall consider the Day-1 volumetrics and corresponding infrastructure sizing specified in the RFP and propose an appropriately sized solution with optimal resource requirements. ATS/AMC/Support and all other applicable cost items specifically mentioned in the prescribed BoM/TCO shall be factored into the commercial proposal. Any additional procurement required over and above the prescribed sizing and volumetrics shall be considered on a pro-rata basis, based on the unit rates/quantities quoted in the Commercial BoM.
1889	Pg-136	Descope	Section 11	The Bank reserves the right to reduce or descope solution components before award.	Kindly clarify the minimum guaranteed scope or minimum order value, if any, and whether the bidder may revise the unit rates if the Bank descopes complete solution categories before award.	Please refer addendum for revised clause.
1890	Pg-140–158	SLA and Penalties	Section 13	SLAs and penalties apply to availability, incidents, response, resolution, operations, and service delivery.	Kindly clarify the penalty calculation methodology, monthly cap, aggregate liability cap, exclusions for Bank dependencies, planned maintenance, force majeure, third-party outages, and events caused by the Bank or other vendors.	No Change, Please be guided by the RFP
1891	Pg-140–157	SLA	13.1	SLA requirements apply to the complete solution and services.	Kindly clarify the availability measurement method, monitoring source, maintenance-window treatment, planned downtime allowance, and whether availability will be calculated separately for each solution or as an overall platform availability.	No Change, Please be guided by the RFP
1892	Pg-157–158	Penalties	13.2–13.3	Penalties and at-risk amounts are prescribed in the RFP.	Kindly clarify whether penalties and at-risk amounts are cumulative, whether both may be applied for the same service-level breach, and the maximum aggregate deduction permissible in a billing period.	The At-Risk Amount is a contractual performance mechanism and shall be withheld/adjusted in accordance with the applicable performance requirements specified in the RFP. It shall not automatically be treated as an additional penalty or Liquidated Damages (LD). Any withholding, adjustment or recovery under the At-Risk Amount shall be accounted for within the overall 10% penalty/LD cap specified in Section 13.2 and shall not be over and above such cap.
1893	Pg-159–168	Terms and Conditions	Section 14	The RFP contains assignment, subcontracting, indemnity, liability, termination, audit, and other contractual provisions.	Kindly request the Bank to confirm that the bidder's aggregate liability will be limited to the total contract value or another mutually agreed amount, except for fraud, willful misconduct, confidentiality breach, and infringement of intellectual-property rights.	No Change, Please be guided by the RFP
1894	Pg-161	DPDP Compliance	14.8	The bidder must comply with the Digital Personal Data Protection Act and applicable privacy requirements.	Kindly clarify the parties' respective roles as Data Fiduciary and Data Processor and provide the Bank's required data-processing agreement, security schedule, breach-notification timeline, and cross-border transfer conditions.	No Change, Please be guided by the RFP
1895	Pg-163	Make in India	14.14	Compliance with Make in India/local-content requirements is required.	Kindly clarify the applicable local-content threshold, calculation methodology, required certification format, and whether cloud subscription, OEM software, hardware, and managed services will be evaluated separately for local content.	No Change, Please be guided by the RFP
1896	Pg-256–262	Sizing and Volumetrics	Annexure 21	Solution-wise sizing includes SIEM, SOAR, UEBA, XDR, NDR, VA, ITDR, AST, CSPM, CNAPP, CWPP, and CTEM.	Kindly confirm the basis for the stated quantities, including whether they represent current inventory, initial deployment quantities, peak requirements, or the minimum licensed quantities for the complete contract term.	Details shall be shared with successful bidder
1897	Pg-258	Volumetrics	Annexure 21	SIEM requirement is 50,000 sustainable EPS/2.06 TB/day scalable to 75,000 EPS/3.09 TB/day at DC/DR.	Kindly clarify whether 50,000 EPS/2.06 TB/day is required at each of DC and DR independently or whether it represents the aggregate capacity across both locations.	Please refer addendum for the revised clause
1898	Pg-258–260	Volumetrics	Annexure 21	UEBA requires 50,000 sustainable EPS/2.06 TB/day scalable to 75,000 EPS/3.09 TB/day and 12,000 endpoint users scalable to 16,000.	Kindly clarify whether UEBA must ingest the full SIEM volume independently or whether UEBA may consume relevant normalized events and telemetry from SIEM/XDR without duplicate ingestion and licensing.	Please refer to the relevant Addendum for this clause.
1899	Pg-258–260	Volumetrics	Annexure 21	XDR is required for 12,000 users scalable to 14,000; ITDR is required for 12,000 users/endpoints scalable to 16,000.	Kindly clarify the definitions of "user," "endpoint," "protected user," and "protected endpoint," and confirm whether service accounts, shared accounts, servers, mobile devices, and inactive identities are included.	user wrt to XDR here refers to activie business users/desktops in bank's environment
1900	Pg-258–260	Volumetrics	Annexure 21	AST requires an enterprise SAST license with unlimited applications/scans/lines of code and 30 users, and DAST for at least 25 web-facing applications.	Kindly clarify whether the unlimited SAST entitlement includes third-party SCA, container scanning, IaC scanning, mobile scanning, API scanning, and developer seats, or whether these are separate license metrics.	No Change, Please be guided by the RFP
1901	Pg-260	Volumetrics	Annexure 21	Decoy solution must cover at least 200 applications, networks, and devices with 50 segments across DC and DR.	Kindly clarify whether the requirement is for 200 simultaneously active decoys or 200 assets that may be rotated over the contract period.	Please refer addendum for revised clause.
1902	Pg-261	Data Retention	Annexure 21.3	Backup retention includes daily incremental, weekly full, monthly full, and long-term storage requirements.	Kindly provide the complete retention table, as the visible retention schedule appears incomplete, and clarify retention periods for each solution, including raw logs, processed data, configurations, reports, and audit trails.	Please refer addendum for revised clause.
1903	Pg-261–262	Data Retention	Annexure 21.3	Primary, backup, long-term, replication, snapshot, and operational-headroom requirements must be included in sizing.	Kindly confirm the required annual data-growth percentage, compression assumptions, deduplication assumptions, backup type, replication mode, and storage utilization threshold to be used for sizing.	Please refer addendum for revised clause.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1904	Pg-263–264	Client References	Annexure 22	Client references require project details, solution details, commercial value, status, and supporting documents.	Kindly confirm whether the client-reference format may be signed by an authorized client representative or supported by a client-issued document where the client is unable to sign the prescribed format.	Pleae be guided by the RFP
1905	Pg-267	Proposed Resources	Annexure 24	CVs must include qualifications, certifications, experience, and project-specific relevance.	Kindly clarify whether resources may be proposed as shared subject-matter experts across multiple solution components, provided that the required availability and SLA obligations are met.	No Change, Please be guided by the RFP The Resource requirement given in the RFP is minimum mandatory requirement that is to be deployed. It includes both DC & DR. Bidder can propose the manpower over and above if required.
1906	Pg-268–273	Mandatory Reports	Annexure 25	Multiple daily, weekly, monthly, quarterly, annual, incident-based, and regulatory reports are mandatory deliverables.	Kindly clarify the required report format, delivery mechanism, data granularity, retention period, approval workflow, and whether reports generated through integrated dashboards will be accepted in lieu of separately developed reports.	Pleae be guided by the RFP
1907	Pg-268–273	Mandatory Reports	Annexure 25	Reports include MITRE ATT&CK coverage, detection effectiveness, false positives, threat hunting, exposure, incident RCA, executive cyber risk, and maturity assessment.	Kindly confirm whether the Bank will provide the required business context, asset criticality, application ownership, risk classification, and control mapping necessary to generate these reports accurately.	Pleae be guided by the RFP
1908	Pg-268–273	Mandatory Reports	Annexure 25	Annual SOC Effectiveness Maturity Assessment and strategic cyber-threat outlook are required.	Kindly clarify the maturity framework, assessment methodology, evaluation criteria, and expected deliverables for the annual SOC maturity assessment and cyber-threat landscape outlook.	Detailed methodology and deliverables shall be agreed with the Bank before the assessment.
1909	101	10.2 Eligibility Criteria Sl.no:04		The bidder should have a minimum average turnover of INR 500 crore per annum in India during the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth. Note – In case of MSMEs only, the turnover may be relaxed subject to meeting the quality and technical specifications.	The bidder should have a minimum average turnover of INR 450 crore per annum in India during the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth. Note – In case of MSMEs only, the turnover may be relaxed subject to meeting the quality and technical specifications.	No Change, Please be guided by the RFP
1910	103	10.2 Eligibility Criteria Sl.no:6		Bidder must have at least enrolled manpower (on bidder's payroll) of 100 experienced employees skilled in areas of Cyber security.	Bidder must have at least enrolled manpower (on bidder's payroll) of 50 experienced employees skilled in areas of Cyber security.	No Change, Please be guided by the RFP
1911	106	10.2 Eligibility Criteria Sl.no:8		Bidder should have supplied, installed and maintained (or under maintenance) any three (3) of the below solutions in any one PSU/PSE/ Government Organizations / BFSI/Telecom provider in India a. SOAR b. UEBA c. Extended Detection & response (XDR)/ Endpoint Detection & response (EDR) d. Network Detection & response (NDR)/Network Behaviour Anomaly Detection (NBAD) e. Threat Intelligence Platform f. Vulnerability Assessment/Vulnerability management g. Identity Threat Detection & response h. Decoy/Honeypot/Deception i. Application security testing tool (DAST or SAST) j. Cloud Security Posture Management (CSPM) k. Cloud-Native Application Protection Platform (CNAPP) l. Cloud Workload Protection Platform (CWPP) m. Continuous Threat Exposure Management (CTEM) Note: - Experience of solutions can be shown in single /multiple Clients/ work orders meeting the above criteria A bidder's experience in supplying and installing a solution will be considered regardless of	Bidder/OEM should have supplied, installed and maintained (or under maintenance) any three (3) of the below solutions in any one PSU/PSE/ Government Organizations / BFSI/Telecom provider in India a. SOAR b. UEBA c. Extended Detection & response (XDR)/ Endpoint Detection & response (EDR) d. Network Detection & response (NDR)/Network Behaviour Anomaly Detection (NBAD) e. Threat Intelligence Platform f. Vulnerability Assessment/Vulnerability management g. Identity Threat Detection & response h. Decoy/Honeypot/Deception i. Application security testing tool (DAST or SAST) j. Cloud Security Posture Management (CSPM) k. Cloud-Native Application Protection Platform (CNAPP) l. Cloud Workload Protection Platform (CWPP) m. Continuous Threat Exposure Management (CTEM) n.SIEM Note: - Experience of solutions can be shown in single /multiple Clients/ work orders meeting the above criteria A bidder's experience in supplying and installing a solution will be considered regardless of when the installation was completed. Even if the installation was completed more than five years ago, it will still qualify, provided that the same bidder is currently maintaining that solution or has carried out its maintenance at	Please refer addendum for the revised clause
1912	129	10.3 Technical Evaluation Criteria Sl.no:1		Bidder should have supplied, installed and maintained (or under maintenance) the below solutions in any one PSU/PSE/ Government Organizations / BFSI/Telecom provider in India 1. SOAR 2. UEBA 3. Extended Detection & response (XDR)/ Endpoint Detection & response (EDR) 4. Network Detection & response (NDR) 5. Threat Intelligence Platform 6. Vulnerability Assessment / Vulnerability Management 7. Identity Threat Detection & response (ITDR) 8. Decoy/Honeypot/Deception 9. Application security testing tool (DAST/SAST) 10. CSPM	Bidder/OEM should have supplied, installed and maintained (or under maintenance) the below solutions in any one PSU/PSE/ Government Organizations / BFSI/Telecom provider in India 1. SOAR 2. UEBA 3. Extended Detection & response (XDR)/ Endpoint Detection & response (EDR) 4. Network Detection & response (NDR) 5. Threat Intelligence Platform 6. Vulnerability Assessment / Vulnerability Management 7. Identity Threat Detection & response (ITDR) 8. Decoy/Honeypot/Deception 9. Application security testing tool (DAST/SAST) 10. CSPM	Please refer addendum for the revised clause
1913	35 of 122	XDR	4.13	The goal is to minimize the attack surface by continuously monitoring, updating, and provide compensatory controls for vulnerabilities and exploits in the endpoints	We request to modify this clause as below "The goal is to minimize the attack surface by continuously monitoring, updating, and provide visibility for vulnerabilities and exploits in the endpoints" Justification: The term "visibility" is outcome-focused and technology-agnostic, allowing solutions to detect and report vulnerabilities through various mechanisms (signatures, behavioral analysis, real-time scanning, etc.), whereas "compensatory controls" is overly prescriptive and implies specific mitigation techniques that may not be applicable to all vulnerability types or endpoint environments. Changing to "visibility" maintains the security intent while enabling bidders to propose diverse, fit-for-purpose solutions without unnecessary implementation constraints.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1914	35 of 122		12	The proposed solution must provide protection against malicious AI application tampering on the endpoints	We request to modify this clause as below "The proposed solution must provide protection against malicious applications tampering on the endpoints" Justification:The "AI" qualifier is overly specific and may exclude non-AI malware threats, creating coverage gaps. The broader term "malicious application tampering" aligns with industry-standard endpoint protection language and ensures comprehensive threat protection regardless of the attack vector or technology employed.	No Change, Please be guided by the RFP
1915	36 of 122		15	The proposed XDR solution must provide comprehensive activity data management and search capabilities, including receiving activity data in the form of telemetry, and metadata; feature for automatic query runs and email notifications; threat matching features using Boolean Logic and other criteria; and options to export, import, delete, and share saved search queries.	We request to modify this clause as below: The proposed XDR solution must provide comprehensive activity data management and search capabilities, including receiving activity data in the form of telemetry, and metadata; feature for automatic query runs and email notifications; threat matching features using Boolean Logic and other criteria; and options to export, delete, and share saved search queries. Justification:The "import" functionality is not a core operational requirement for XDR activity data management. The primary requirements are exporting queries for backup/sharing, deleting obsolete queries, and sharing queries among team members—all of which are standard XDR capabilities. Import functionality introduces unnecessary complexity, potential security/governance risks from external query sources, and is not universally supported across commercial XDR solutions, thereby limiting vendor options unnecessarily	No Change, Please be guided by the RFP
1916	36 of 122		22	The solution should offer options to leverage anti-malware and anti-spyware components stored locally on agents, or signatures stored in-the-vendor cloud	From the operational context and use cases for each deployment option, ensuring continuity of threat protection in all connectivity scenarios. By explicitly defining "when offline" (local components) and "when online" (cloud signatures), the clause removes ambiguity regarding the solution's capability to maintain protective coverage during network disconnections while leveraging updated threat intelligence when connectivity is available We request to modify this clause as below "The solution should offer options to leverage anti-malware and anti-spyware components stored locally on agents when offline, or signatures stored in-the-vendor cloud when online."	No Change, Please be guided by the RFP
1917	36 of 122		29	The solution Device Control capability must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The solution Device Control capability must support Network Devices, USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, time based device control capabilities allowing admin to define the policy specifically for the endpoint operating systems (Windows 10, 11 or higher).	We request to modify the clause as below: The solution Device Control capability must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The solution Device Control capability must support USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, allowing admin to define the policy specifically for the endpoint operating systems (Windows 10, 11 or higher)to allow the devices as required. Justification: Network Devices are typically managed through enterprise network security controls and firewalls rather than endpoint Device Control, and time-based controls create unnecessary operational complexity and maintenance overhead. The modified clause focuses on high-risk local device vectors (USB, Mobile Storage, Bluetooth, Modems) that pose direct security threats to endpoints, while allowing flexibility for organizations to enable specific devices based on business requirements.	No Change, Please be guided by the RFP
1918	37 of 122		43	The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature or through seamless integration with a third-party sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data	We request to amend this clause as below: The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data. Justification: To ensure operational independence and reduce implementation complexity, the organization requires native sandbox functionality built into the core solution rather than relying on third-party integrations, which introduce external dependencies, potential single points of failure, and increase support overhead. This modification mandates that bidders deliver complete sandboxing capability as an integrated component from day 1, ensuring seamless functionality, consistent vendor accountability, and simplified maintenance and support operations without external vendor coordination.	Please refer addendum for revised Clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1919	38 of 122		57	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	We request to amend this clause as below: The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture or 99.9% availability SLA distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead. Justification: The modification provides architectural flexibility while maintaining the Bank's core availability objective. Not all qualified SaaS vendors employ Active-Active multi-AZ architecture; however, industry-standard 99.9% SLA meets enterprise-grade requirements and enables broader vendor participation without compromising operational resilience. This alternative approach is vendor-agnostic, measurable, and backed by contractual guarantees rather than architectural prescriptions.	Please refer Addendum for revised clause
1920	37 of 122		42	The proposed solution should provide recommended actions to address and mitigate threats detected on endpoints. These remediation suggestions should be informed by forensic data collected from endpoints and detailed analysis performed by the solution to enhance threat response and resolution.	To ensure accurate cost proposals and licensing calculations, please clarify the estimated forensics data volume requirements: a) What is the expected monthly forensics data volume (in GB) that the solution must support? b) What is the planned retention period for forensics data? c) Does this volume include forensics data from all sources (endpoints, servers, cloud workloads, network) or specific sources only? This clarification will enable all bidders to calculate appropriate licensing models and provide consistent cost estimates	Details shall be shared with the successful bidder
1921	54 of 122	Cloud Security	4	The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud envirionment like AWS/Azure/GCP/Meghdoot, AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.	We request to modify this clause as below The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud envirionment like AWS/Azure/GCP/ AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports. Justification: Meghdoot is a comprehensive open-source cloud suite, but bringing it up to PSB requirements demands significant development and integration effort. To be effective, the target cloud environment must be seamless, eliminating the overhead of custom modifications.	Please refer addenudm for revised clause The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud envirionment like AWS/Azure/GCP, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.
1922	Addition of Point as recommendatio n	Cloud Security	To be Added in Cloud Security	The proposed solution should also support the File scanning with no limitation on file/object type or size covering application across organisation. This should include but is not limited to Amazon Simple Storage Service (S3), Amazon FSx amd Amanzon Elastic File System.	Benefit to PSB: Comprehensive file scanning eliminates critical security blind spots across the organization's cloud storage infrastructure, ensuring no malware, ransomware, or sensitive data can be inadvertently stored in S3, FSx, or EFS without detection. By removing file type and size limitations, the solution prevents attackers from bypassing scanning through obfuscation or leveraging uncommon formats, while the multi-storage coverage consolidates security posture across diverse AWS storage services under a single unified policy. This provides unified threat visibility, enables regulatory compliance (HIPAA, PCI-DSS, GDPR), prevents data exfiltration, and protects against insider threats and supply chain compromises affecting cloud-stored data—significantly reducing the risk of ransomware attacks, compliance violations, and unauthorized data exposure.	No Change, Please be guided by the RFP
1923	page 30 of 273	Extended Detection & Response (XDR)	5	Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Cloud (SaaS): HA Deployment aligned with the SLA, RTO & RPO (Refer Section 13). Management Console: Deployed at both Primary and Secondary sites	We request to amend this clause as below: Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Cloud (SaaS): HA Deployment aligned with the SLA, RTO & RPO (Refer Section 13). Justification: In Appendix 1A clause 27 under XDR explicitly mention for SaaS "ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead" Though it's a SaaS based the management console cannot be deployed at both primary and secondary sites.	Please refer addendum for revised clause
1924	page 31 of 273	Cloud Workload Protection Platform (CWPP)	13	Cloud (SaaS): Deployment aligned with the SLA, RTO & RPO (Refer Section 13).. Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Management Console: Deployed at both Primary and Secondary sites	We request to amend this clause as below: Cloud (SaaS): Deployment aligned with the SLA, RTO & RPO (Refer Section 13).. Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Justification: For SaaS solution the management console cannot be deployed at banks primary & secondary site	Please refer addendum for revised clause
1925	Page 38 of 122 & Page 38 of 122	XDR	22 to 35	These points are duplicate need to be removed	These points are duplicate need to be removed	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1926	30	7.2.1 Solutions – Master Deployment Matrix	#8. Vulnerability assessment (VA) & vulnerability lifecycle management	Bank Location: Standalone at DC and Standalone at DR. Management Console: Deployed at both DC and DR	As per this RFP Technical Specification of VA & VLM,document #1788963129, #12 "The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and failover capabilities" where the 7.2.1 of suggests standalone deployment at DC, DR and console availablity at both DC and DR. These two partially contradict each other. We request you to kindly confirm if standalone VA & VM in DC and DR are expected to function independently. Maintaining two standalone environments with both consoles accessibility will lead to duplication of vulnerabilities, configuration efforts and it will cost upto 2X in terms of licensing. Though its not clear but we assume that you need one VM in DC and one in DR where primary one shares configuration backup on secondary and secondary can take over when the primary goes down, the primary VM solution should be able to scan both the DCs and vice-versa. If this understanding is correct, kindly update the clause as following - 'The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and active-cold standby failover capabilities where only one active console shall be accessible at a time'.	No Change, Please be guided by the RFP
1927	260	16.21.2 Volumetrics-Solution-wise Requirements	10 Vulnerability Assessment & Management (VA-VM) Minimum Numbers of IPs: 4000	10 Vulnerability Assessment & Management (VA-VM) Minimum Numbers of IPs: 4000	As per the RFP #1788963158, page 257 16.21.1 Current IT assets, P&SB has 2500 servers, 300 DB, 200 Apps, 12000 endpoints/desktops and 7200 routers and switches whereas the VA/VM IP coverage is mention as "Minimum" 4000. We seek your guidance and confirmation on the final count of assets/IPs you need coverage from day #1, given "minimum" count may lead to each bidder proposing seperate numbers and very likely excluding important assets from highly important VA & VM exercise. Without a defined and finite asset count, bidders cannot be compared on a like-for-like basis as the ones concerned about the VA/VM security posture of the infra will propose to cover more IPs/Assets while some may cover bare minimum and appear more competitive. We request you to kindly provide the final IP count required for VA/VM from day #1 considering the licenses are bound to assets and deleting the asset will delete all historic vulnerability and trends data, deleted asset will not cover alerts, ITSM integration and cannot be considered as part of VM exercise. As per the CERT'in recommendations (https://www.cert-in.org.in/PDF/guidelinesgovtentities.pdf) as well as industry best practices, entire ICT infrastructure should be part of the vulnerability management exercise and network device inclusion is absolute must given these are critical assets and in some zones exposed directly to internet.	No Change, Please be guided by the RFP
1928	38	On premises deployment of solutions	Storage Capacity & Sizing	• The Bidder shall provide detailed storage sizing based on expected data/log volumes, peak ingestion rate, retention period, indexing, enrichment, compression, replication, backup, archival and anticipated annual growth. Adequate capacity shall be provisioned for the complete contract period.	As per the RFP #1788963158, storage duration on the primary storage of the solution itself is mention for Cloud/SaaS/Hybrid to be 3 months, same is not clearly specified for VA & VM. Kindly confirm how long should the VA & VM solution retain the asset, vulnerability, logs, activities, historic trend etc. As per CERT-IN it must be 6 months. Kindly confirm if you wish the solution to retain this info on its own primary storage to be for 6 months or less.	Please refer addendum for revised clause
1929	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - VA-VM	VA-VM S.No. 9	Each scanning engine shall support web application security assessment together with traditional infrastructure vulnerability and configuration/compliance assessment. The solution shall identify vulnerabilities, missing patches, insecure configurations, and compliance deviations, and generate comprehensive reports containing risk severity, evidence of findings, affected assets, and remediation recommendations to support security governance, audit, and regulatory compliance.	While its possible to perform this via VA VM solution with additional WAS/DAST license, this will be a duplication of solution given you are already asking for seperate 'Application Security Testing Tool'. Hence, we request you to kindly move the 'Web application security assessment' from VA & VM requirements to DAST as this is a DAST requirement and may unnecessorily require to duplicate the licenses, solution and hardware.	No Change, Please be guided by the RFP
1930	Functional Compliance Sheet pp.48-51 (Appendix 1A)	Appendix 1A - VA-VM	VA-VM S.No. 36-52 and S.No. 61-77; S.No. 87 and S.No. 89	All technical compliances of VA-VM S.No. 36-52 and S.No. 61-77; S.No. 87 and S.No. 89	S.N 61-77 are likely duplicates of S.N 36 to 52 with minor changes. Request you to kindly review and confirm if this is intentional or typo. If not intentional, kindly remove duplicates to have the score calculated accordingly.	No Change, Please be guided by the RFP
1931	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 12	The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and failover capabilities.	VM solution is not an inline and always active solution.VM solutions across the industry do not have failovers similar to inline solutions such as firewalls. Hence, we request you to kindly consider the failover scenario as active - cold standby with documented backup-restore and a controlled switchover in place of automatic console failover. We request you to kindly update the clause as - The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and failover capabilities either automatically or using manual and controlled backup restore.	No Change, Please be guided by the RFP
1932	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 15	The proposed solution shall support integration with SIEM, SOAR, Threat Intelligence Platforms, NAC, and other security platforms through APIs or standard integration mechanisms.	Kindly share details (Vendor/Model/Version) of the SIEM, SOAR, TIP and NAC solution you would want to integrate with for us to identify the availablity of standard or API based integration and accordingly finalize the deployment efforts.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1933	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 16	The proposed solution shall integrate with Privileged Access Management (PAM) solutions for secure credential management during authenticated scans.	Kindly share details (Vendor/Model/Version) of the PAM solution you would want to integrate with for us to identify the availablity of integration and also identify the deployment efforts.	Bank is currently procuring PAM solution through separate RFP.
1934	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 17	The proposed solution shall integrate with IT Service Management (ITSM) and ticketing platforms for automated vulnerability tracking and remediation workflows.	Kindly share details (Vendor/Model/Version) of the ITSM solution you would want to integrate with for us to identify the availablity of standard or API based integration and accordingly finalize the deployment efforts.	ITSM - Manage Engine
1935	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 29	The proposed solution shall support vulnerability assessment and compliance reporting aligned with PCI DSS requirements.	We request you to kindly confirm whether you only require to perform PCI DSS internal scanning and reporting on-premises or you also require the PCI- ASV attestation. If Attestation is required, kindly share the exact asset count for which the attestation is needed and how many attestations are to be submitted within 1 year.	No Change, Please be guided by the RFP
1936	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 42	The solution shall support vulnerability assessment of VMware ESXi, Hyper-V, Nutanix AHV, Kubernetes, OpenShift and container platforms.	We request you to kindly confirm whether you need the OS and platform vulnerability assessment of these container solutions or you need a comprehensive container security solution with the ability to identity vulnerabilities of images, registries and their components. If you need comprehensive container security assessment, we request you to kinly move this required to CNAPP solution as its usually part of cloud security solutions and not VM solution.	No Change, Please be guided by the RFP
1937	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 45	The solution shall integrate with enterprise CMDB, ITSM, SIEM, SOAR, PAM and NAC platforms through secure REST APIs.	Kindly share details (Vendor/Model/Version) of the required solutions you would want to integrate with for us to identify the deployment efforts.	Please refer addendum for the revised clause Details shall be shared with successful bidder
1938	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 47	The solution shall support Multi-Factor Authentication (MFA), LDAP, Active Directory, SAML 2.0 and OpenID Connect authentication.	We request you to kindly remove the OpenID and update the clause as following - The solution shall support Multi-Factor Authentication (MFA via SAML and/or LDAP), LDAP, Active Directory, SAML 2.0.	No Change, Please be guided by the RFP
1939	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 48	The solution shall support secure encrypted communication using TLS 1.3 and cryptographic modules compliant with FIPS 140-3 or equivalent internationally recognized standards.	We request you to kindly allow the FIPS 140-2 or equivilent solution transitioning to FIPS 140-3 to participate and update the clause as following - The solution shall support secure encrypted communication using TLS 1.3 and cryptographic modules compliant with FIPS 140-2 or FIPS 140-3 or equivalent internationally recognized standards.	Please refer addendum for revised clause
1940	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 51	The solution shall identify internet-facing assets and continuously monitor externally exposed services.	We request you to kindly remove this clause as its an ASM(Attack Surface Management) requirements which is already asked separate service based solution of the RFP.	Please refer the addendum for revised clause
1941	Functional Compliance Sheet p.49 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 56	The solution shall support digitally signed and password-protected reports with configurable retention and archival.	We request you to kindly update the clause as following - The solution shall support password-protected reports with configurable retention and archival.	Please refer addendum for revised clause
1942	Functional Compliance Sheet p.49 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 60	The solution shall provide comprehensive REST APIs and webhook support for automation and integration with enterprise security platforms.	We request you to kindly update the clause as following - The solution shall provide comprehensive REST APIs or webhook support for automation and integration with enterprise security platforms.	Please refer addendum for revised clause
1943	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 87	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	We request you to kindly remove this clause from VM VM and move it to CTEM as this is a CTEM requirement, a solution that can be cloud/SaaS based. Given the data soveraginity and sensitivity of bank's vulnerabilities data, the platform is correctly requested to be on-prem which shall also be able to function without any internet connectivity. Hence, AI powering the on-prem application to achieve all the listed items is not viable. We request you to kindly remove this point and move it to CTEM.	Please refer the addendum for revised clause
1944	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 88	Unified, correlated findings intelligence. Every scanning engine — across web, API, network and host, cloud, containers, mobile, source code, device configuration and identity — reports into a single normalized findings model..	This is a CTEM requirement as VM solution won't perform VA of source code, identity etc. Kindly move this from VA VM to CTEM requirements.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1945	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 89	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	This is a duplicate of S.N. #87, kindly remove it.	Please refer the addendum for revised clause
1946	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 90	Mobile Application Security Testing: The proposed solution shall support static security analysis of Android and iOS mobile application packages, including APK/AAB and IPA formats, and shall provide security assessment mapped to recognized mobile application security standards and methodologies such as OWASP MASVS and MASTG.	This is not part of any VA/VM solution in industry and belongs to application security testing. We request you to kindly move this to 'Application Security Testing Tool'.	No Change, Please be guided by the RFP
1947	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 91	White-Label Reporting and Approval Workflow: The proposed solution shall support customizable/white-label security assessment reports, including organization-specific branding and configurable report content. The solution shall support role-based maker-checker workflow for report generation, review, approval, and controlled release of finalized reports.	We request you to kindly update the clause as following - White-Label Reporting and Approval Workflow: The proposed solution shall support customizable/white-label security assessment reports, including organization-specific branding and configurable report content. The solution shall support role-based access for report generation, review of the finalized reports.	Please refer addendum for the revised clause White-Label Reporting and Approval Workflow: The proposed solution shall support customizable/white-label security assessment reports, including organization-specific branding and configurable report content. The solution shall support role-based or maker-checker workflow for report generation, review, approval of finalized reports.
1948	92	7.18.1 Compute Infrastructure	10. Non-production:	10. Non-production: a) The non-production environments should have the same software and hardware setup as deployed in production environments meeting all RFP requirements.	While this clause suggests the hardware and software setup of non-prod to be same, "16.21 Annexure 21: Sizing/Volumetrics, Data Retention and Current Infrastructure" suggests the VM based solution to have minimum 10% size. Kindly confirm if the 10% requirement of non-production infra is for only licenses whereas the hardware specs are to be identical to prod or both the licenses as well as hardware/software specs to be 10% of the production infra. Also kindly confirm if the non-production is to be setup only at DC or DC as well as DR.	Please refer addendum for the revised clause
1949	Functional Compliance Sheet pp.47-51 (Appendix 1A)	Appendix 1A - VA-VM	TOTAL MARKS row and S.No. 1 to 94	TOTAL MARKS - 850	While the VA-VM section contains 94 scoreable clauses, each carrying Maximum Marks of 10, which totals 940 marks, whereas the TOTAL MARKS row of the section states 850. We request you to kindly publish the corrected total and confirm the marks allocated per clause, so that bidders can compute the Respective Solution Compliance required by the Appendix 1A summary sheet consistently.	Please refer addendum for the revised clause
1950	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 19, 20, 43 and 44 (missing) and TOTAL MARKS row	CNAPP section is numbered from S.No. 1 to S.No. 60; however S.No. 19, 20, 43 and 44 do not appear in the sheet. TOTAL MARKS - 560.	The CNAPP section is numbered up to S.No. 60 but S.No. 19, 20, 43 and 44 are not present, leaving 56 scoreable clauses which, at 10 marks each, reconciles to the stated TOTAL MARKS of 560. We request you to kindly confirm whether these four clauses have been intentionally deleted or have been inadvertently omitted from the published sheet. If clauses exist against these serial numbers, kindly publish them along with the revised TOTAL MARKS; if they have been deleted, kindly re-issue the sheet with continuous numbering so that bidders' compliance responses and score computation remain traceable to the Bank's evaluation sheet.	Please refer addendum for the revised clause
1951	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 16	The solution shall support integration with relevant source-code repositories, development tools, build systems, CI/CD platforms and security workflows, either natively or through supported connectors/APIs.	A CNAPP integrates with source-code repositories and CI/CD platforms for Infrastructure-as-Code (IaC), container image and cloud-configuration assessment. It does not act as a source-code security testing tool, which is the function of the separately procured 'Application Security Testing Tool' in this RFP. We request you to kindly update the clause as following - "The solution shall support integration with relevant source-code repositories, development tools, build systems, CI/CD platforms and security workflows, either natively or through supported connectors/APIs, for the purpose of Infrastructure-as-Code, container image and cloud configuration assessment."	No Change, Please be guided by the RFP
1952	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 17 and S.No. 18	S.No. 17 - The solution shall identify security risks and known vulnerabilities associated with third-party, open-source and externally sourced software components and dependencies used by cloud-native applications. S.No. 18 - The solution shall provide visibility into application dependencies and software components and shall identify affected applications where a vulnerable component or dependency is detected.	Identification of third-party/open-source components and application dependencies is a Software Composition Analysis (SCA)/SBOM capability which belongs to the 'Application Security Testing Tool' scope already sought separately in this RFP, and requiring it again under CNAPP will lead to duplication of licences and cost without additional security benefit to the Bank. We request you to kindly either move these clauses to the Application Security Testing Tool requirements, or update them as following - "The solution shall identify known vulnerabilities in third-party and open-source software components and dependencies present within container images, registries and cloud workloads assessed by the platform, and shall identify the affected cloud-native applications/components."	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1953	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 24	The solution shall provide security visibility for cloud-native APIs and application interfaces, including risks related to exposure, authentication, authorization, access control and relevant configurations, where supported.	Discovery and security assessment of application APIs (including authentication/authorization testing of API endpoints) is the function of a dedicated API Security/API posture solution, and is not a native capability of CNAPP platforms. CNAPP platforms provide visibility of cloud-native API gateway and managed API service configurations and their exposure. We request you to kindly update the clause as following - "The solution shall provide security visibility for cloud-provider API gateway/managed API services and application interfaces discovered from the cloud control plane, including risks related to public exposure, authentication/authorization configuration and access control settings, where supported by the respective cloud platform."	No Change, Please be guided by the RFP
1954	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 26	The solution shall provide visibility into application access to sensitive or critical data and identify security risks arising from inappropriate application access, exposure or relationships, where supported.	As worded, this clause can be read as requiring full Data Security Posture Management (DSPM) with data discovery and classification of the Bank's data stores, which is a separately licensable product category and is not part of a baseline CNAPP. We request you to kindly confirm whether DSPM (data discovery and classification) is intended to be in scope of the CNAPP. If it is not intended, we request you to kindly update the clause as following - "The solution shall provide visibility into application and identity access paths to cloud data stores and shall identify security risks arising from public exposure, excessive access or inappropriate relationships to such data stores, where supported by the respective cloud platform." If DSPM is intended, kindly publish the applicable volumetrics (number/size of data stores) so that bidders can size and price the module consistently.	No Change, Please be guided by the RFP
1955	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 27	The solution shall identify vulnerable application components that are reachable, exposed or potentially exploitable within the application's dependency or relationship graph, where such analysis is supported.	Code-level 'reachability' analysis of a vulnerable function within an application's dependency graph is an SCA/ASPM capability delivered by application security testing tools. CNAPP platforms determine exposure and exploitability from cloud context - internet exposure, network path, identity privilege and attack-path relationships. We request you to kindly update the clause as following - "The solution shall identify vulnerable application components that are internet-exposed, network-reachable or potentially exploitable based on cloud exposure, network path, identity privilege and attack-path relationship analysis, where such analysis is supported by the proposed solution."	No Change, Please be guided by the RFP
1956	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 32	The solution shall provide guided, semi-automated and/or automated remediation capabilities for supported application-security findings.	Fully automated remediation executed directly by a security platform on a production banking cloud environment is generally not permitted under change-management controls, and CNAPP platforms deliver remediation as guided steps and auto-generated remediation artefacts (e.g., IaC fix code/pull requests, CLI commands, policy snippets) which are then applied by the Bank/implementation partner through the Bank's change process. We request you to kindly update the clause as following - "The solution shall provide guided remediation and automatically generated remediation artefacts (such as IaC remediation code, pull requests, CLI commands or policy snippets) for supported application-security findings, which may be applied through the Bank's approved change-management process or through integration with the Bank's SOAR/ITSM platform."	No Change, Please be guided by the RFP
1957	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 59	The solution shall support high availability and service continuity appropriate to the proposed deployment architecture and shall provide mechanisms for recovery of relevant configurations, policies and security information.	Where the CNAPP is delivered as OEM-managed SaaS, high availability, redundancy, backup and disaster recovery are provided by the OEM within the platform and are governed by the OEM's published availability SLA; the Bank cannot be provided Bank-operated HA/DR or restore mechanisms for a SaaS platform. We request you to kindly update the clause as following - "For SaaS-delivered solutions, the OEM shall provide high availability, redundancy and disaster recovery within the platform in line with its published availability SLA, and shall provide mechanisms for export/retrieval of relevant configurations, policies and security information. For on-premises components, if any, the solution shall support HA and documented backup-restore."	Please refer to the addendum: The solution shall support service continuity appropriate to the proposed deployment architecture and shall provide mechanisms for recovery of relevant configurations, policies and security information.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1958	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP - Section scope (S.No. 1 to 50, principally S.No. 1, 6, 7, 8 to 41)	The proposed Cloud Workload Protection Platform (CWPP) shall provide centralized capabilities for protecting, monitoring, detecting, investigating and responding to security threats affecting cloud workloads during runtime. (S.No. 1) and the runtime detection, prevention, response, forensics and threat-hunting clauses at S.No. 6 to 41.	The CWPP section as drafted is predominantly a runtime endpoint/server threat prevention, detection and response (EDR/XDR-class) specification - in-guest malware and ransomware prevention, exploit prevention, host IDS/IPS, file integrity monitoring, process and command-line telemetry, containment actions such as process termination, file quarantine and workload isolation, forensic timelines, process trees and threat hunting. These are delivered by an EDR/XDR agent platform, whereas the CNAPP/CWPP category referenced elsewhere in this RFP delivers agentless workload vulnerability, malware, misconfiguration, identity, secrets and exposure assessment with attack-path context. Given the Bank is separately procuring EDR/XDR and SOC/SIEM capabilities under this very RFP, we request you to kindly clarify and confirm any one of the following, so that bidders are not compelled to bid a second endpoint agent on the same servers: 1. That runtime prevention, containment and forensics requirements of the CWPP section may be met through the Bank's in-scope EDR/XDR platform, with the CWPP providing agentless workload exposure assessment, posture and attack-path context integrated with it; or 2. That the CWPP section may be responded to on a multi-OEM/consortium basis with clear identification of the product meeting each clause (consistent with S.No. 50 of this section); or 3. That the runtime prevention/response clauses be moved	No Change, Please be guided by the RFP
1959	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 2 and S.No. 3	S.No. 2 - The solution shall support protection of workloads deployed across physical, virtual, private-cloud, public-cloud and hybrid-cloud environments, as applicable. S.No. 3 - The solution shall support major public-cloud environments including AWS, Microsoft Azure and Google Cloud Platform, as applicable.	CWPP licensing and sizing depend entirely on the workload inventory in scope, and the clause extends coverage to physical and private-cloud workloads in addition to public cloud. We request you to kindly publish, for the CWPP scope, the workload volumetrics for day #1 and for the contract period - number of physical servers, virtual machines, public-cloud instances (per CSP), container hosts/nodes, Kubernetes clusters and serverless functions - along with the CSP accounts/subscriptions/projects in scope. Kindly also confirm which of these environments are mandatory on day #1, since 'as applicable' may lead each bidder to price a different scope and render the commercial bids non-comparable.	No Change, Please be guided by the RFP
1960	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 8, S.No. 21 and S.No. 22	S.No. 8 - The solution shall detect and prevent, where supported, malware, ransomware, trojans, rootkits and other malicious software or activities affecting protected workloads. S.No. 21 - The solution shall provide protection against ransomware and destructive activities, including detection of abnormal file encryption or mass file modification behavior. S.No. 22 - The solution shall provide exploit detection and/or prevention capabilities for supported workload operating systems and applications.	In-guest prevention of malware, ransomware, trojans and rootkits, behavioural detection of mass file-encryption, and memory/exploit prevention require a kernel-level endpoint prevention engine (EDR/EPP) and are not functions of an agentless cloud workload protection platform, which performs malware and vulnerability detection through workload snapshot/disk analysis without in-line blocking. We request you to kindly move these clauses to the EDR/XDR section of the RFP, or update them as following - "The solution shall detect malware, ransomware, trojans, rootkits, malicious files and destructive activity affecting protected workloads through agentless and/or agent-based assessment, and shall support prevention/blocking natively or through integration with the Bank's EDR/XDR platform."	S.No. 8- No Change, Please be guided by the RFP S.No. 21- No Change, Please be guided by the RFP S.No. 22- No Change, Please be guided by the RFP
1961	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 9 to S.No. 14	S.No. 9 to 14 - monitoring of process execution and process behaviour; detection of suspicious process chains and abnormal parent-child relationships; monitoring of command-line execution, scripts and interpreters; detection of Living-off-the-Land techniques; behavioural/heuristic analysis of anomalous activity; and detection of privilege escalation, persistence, lateral movement and credential misuse.	These clauses describe in-guest runtime behavioural telemetry (process, command-line, script and parent-child process monitoring) which is collected by an EDR/XDR sensor and analysed in the SOC/SIEM. A CWPP that assesses workload exposure agentlessly does not generate kernel-level process telemetry. We request you to kindly move these clauses to the EDR/XDR section, or update them as following - "The solution shall provide the specified runtime behavioural detection capabilities natively or through correlation of telemetry from the Bank's EDR/XDR and SIEM platforms, and shall enrich such detections with workload vulnerability, identity, configuration and exposure context." Kindly also confirm that a capability delivered through such integration will not be treated as non-compliant, consistent with the principle already accepted at CNAPP S.No. 53 of this Appendix.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1962	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 15, S.No. 16 and S.No. 17	S.No. 15 - The solution shall monitor relevant network communications involving protected workloads and identify suspicious or unauthorized communication patterns. S.No. 16 - The solution shall identify communication with known or suspected malicious infrastructure, including malicious IP addresses, domains, URLs, command-and-control infrastructure or equivalent threat indicators, where applicable. S.No. 17 - The solution shall provide host/workload-based intrusion detection and/or prevention capabilities for supported operating systems and workloads.	Host-based intrusion detection/prevention and in-line inspection of workload network traffic for command-and-control communication are functions of HIDS/HIPS agents, NDR and NGFW/IPS controls, all of which are separately in scope in this RFP. A CWPP provides network exposure and reachability analysis from cloud configuration (security groups, NACLs, routes, load balancers, public exposure) rather than packet-level inspection. We request you to kindly move these clauses to the EDR/XDR, NDR or NGFW sections as appropriate, or update them as following - "The solution shall identify workload network exposure, reachable paths and unauthorized/high-risk communication paths from cloud network configuration and available flow logs, and shall support identification of communication with known malicious infrastructure natively or through integration with the Bank's EDR/XDR, NDR, NGFW and SIEM platforms."	S.No. 15- No Change, Please be guided by the RFP S.No. 16- No Change, Please be guided by the RFP S.No. 17- No Change, Please be guided by the RFP
1963	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 18 and S.No. 19	S.No. 18 - The solution shall monitor critical files, directories, system objects and configuration elements for unauthorized modification, creation or deletion, where supported. S.No. 19 - The solution shall provide file integrity monitoring for designated critical files, directories and system objects.	File Integrity Monitoring (FIM) requires a resident agent performing real-time file-system event monitoring on the workload and is a standard EDR/host-integrity capability. It is not delivered by an agentless cloud workload protection platform. We request you to kindly move these clauses to the EDR/XDR section, or update them as following - "File integrity monitoring for designated critical files, directories and system objects shall be provided natively or through integration with the Bank's EDR/XDR or host-integrity solution, with the resulting events available for correlation and reporting."	No Change, Please be guided by the RFP
1964	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 20 and S.No. 24	S.No. 20 - The solution shall detect suspicious creation or modification of system accounts, services, scheduled tasks and other persistence mechanisms, where applicable. S.No. 24 - The solution shall support detection and/or prevention of web-shell and other unauthorized application-level persistence mechanisms, where applicable.	Real-time detection of persistence mechanisms and prevention of web-shell execution are runtime endpoint and web application protection (EDR/WAF) functions. A CWPP can identify such artefacts through periodic workload assessment but cannot prevent their execution. We request you to kindly move these clauses to the EDR/XDR and WAF sections respectively, or update them as following - "The solution shall identify unauthorized accounts, services, scheduled tasks, web-shells and other persistence artefacts present on assessed workloads, and shall support real-time detection/prevention natively or through integration with the Bank's EDR/XDR and WAF platforms."	No Change, Please be guided by the RFP
1965	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 23	The solution shall support virtual patching or equivalent compensating protection mechanisms, where applicable, for vulnerabilities for which immediate patching is not feasible.	Virtual patching is enforced by in-line controls - host IPS agents, NGFW/IPS and WAF - all of which are separately procured under this RFP. A workload protection/exposure platform identifies the vulnerability and recommends the compensating control; it does not itself enforce a virtual patch. We request you to kindly remove this clause from the CWPP section as it is already covered by the Bank's NGFW/IPS and WAF requirements, or update it as following - "For vulnerabilities where immediate patching is not feasible, the solution shall identify the exposure, provide risk context and recommend applicable compensating controls, which may be enforced through the Bank's in-line security controls (host IPS, NGFW/IPS, WAF) through supported integration."	No Change, Please be guided by the RFP
1966	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 25, 26, 27 and 28	S.No. 25 - runtime security monitoring and threat detection for containerized workloads; S.No. 26 - runtime protection for Kubernetes workloads including pods, containers and workload processes; S.No. 27 - detection of suspicious behaviour involving containers, pods, workload processes and workload-to-workload communications; S.No. 28 - security monitoring for serverless workloads/functions.	Container and Kubernetes runtime protection requires a privileged runtime sensor (e.g., eBPF/DaemonSet-based) on every node, which materially differs from the container and Kubernetes security posture, image/registry scanning, admission control and Kubernetes misconfiguration and RBAC assessment delivered by a CNAPP/CWPP. We request you to kindly clarify whether the Bank requires (a) container/Kubernetes runtime sensor-based prevention or (b) container and Kubernetes security posture with image, registry, IaC, admission-control and RBAC assessment plus runtime detection through the Bank's EDR/XDR on the worker nodes. We request you to kindly permit option (b) and update the clauses to allow the capability to be delivered through posture assessment, admission control and integration with the Bank's EDR/XDR and SIEM, failing which the clause is restrictive to a small subset of OEMs. Kindly also publish the number of Kubernetes clusters, nodes and serverless functions in scope for sizing.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1967	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 29 and S.No. 30	S.No. 29 - The solution shall support agent-based and/or agentless protection mechanisms, as applicable to different workload types and supported environments. S.No. 30 - Where an agent is required, the solution shall provide mechanisms for secure deployment, centralized management, health monitoring and controlled upgrade of the workload protection agent.	We note and appreciate that S.No. 29 permits agentless mechanisms. However, several other clauses in this section (S.No. 8 to 41) are achievable only through an in-guest agent, which contradicts the option provided in S.No. 29. We request you to kindly confirm that an agentless-first architecture, supplemented where required by the Bank's EDR/XDR agent already deployed on the workloads, will be accepted as compliant against this section, and that S.No. 30 shall apply only where the bidder proposes its own agent. Kindly also confirm that no additional agent is mandated on workloads that already carry the Bank's EDR/XDR agent, in view of performance and change-management impact on production banking workloads.	No Change, Please be guided by the RFP
1968	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 32 and S.No. 33	S.No. 32 - The solution shall support configurable response actions for detected threats, including alerting, blocking, process termination, file quarantine, workload isolation or other equivalent containment actions, as applicable. S.No. 33 - The solution shall provide workload isolation or containment capabilities to limit the impact or spread of a confirmed or suspected compromise, where supported.	Process termination, file quarantine and host/network isolation are kernel-level containment actions performed by an EDR/XDR agent. An agentless workload protection platform performs cloud-control-plane actions (such as snapshotting, tagging, security-group/identity restriction) and orchestrates containment through the Bank's EDR/XDR and SOAR. We request you to kindly move these clauses to the EDR/XDR section, or update them as following - "The solution shall support configurable response actions for detected threats, including alerting, notification, cloud-control-plane containment actions (such as network/identity restriction, snapshot and tagging) natively, and process termination, file quarantine and workload isolation through integration with the Bank's EDR/XDR and SOAR platforms."	S.No. 32 - No Change, Please be guided by the RFP S.No. 33 - No Change, Please be guided by the RFP
1969	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 34, 35, 36 and 37	S.No. 34 - security investigation using process, file, network, user, workload and event-level information; S.No. 35 - historical workload activity and security-event information sufficient for investigation and forensic analysis; S.No. 36 - process-tree or equivalent process-relationship visualization; S.No. 37 - workload-level threat hunting using available security telemetry and configurable search criteria.	Retention of process/file/network event-level telemetry, process-tree reconstruction and telemetry-based threat hunting are EDR/XDR and SIEM functions and require an in-guest sensor. Additionally, these clauses do not specify a retention period, which makes consistent sizing and pricing impossible. We request you to kindly (a) move these clauses to the EDR/XDR and SIEM sections or permit compliance through integration with the Bank's EDR/XDR and SIEM platforms, and (b) if retained under CWPP, publish the mandated telemetry retention period (hot/warm/archive) and the expected daily event volume per workload, so that all bidders size storage and licences on a common basis.	No Change, Please be guided by the RFP
1970	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 38 and S.No. 39	S.No. 38 - The solution shall support identification and searching of Indicators of Compromise (IoCs), including supported hashes, IP addresses, domains, URLs and equivalent indicators. S.No. 39 - The solution shall support integration with external threat-intelligence sources to enhance workload threat detection and investigation.	Retrospective and real-time IoC sweeps across workloads are performed on EDR/XDR telemetry or in the SIEM, where the Bank's threat-intelligence platform feeds are already consolidated under this RFP. We request you to kindly update the clauses as following - "The solution shall support identification and searching of Indicators of Compromise (hashes, IP addresses, domains, URLs and equivalent indicators) against available workload assessment data natively, and across workload runtime telemetry through integration with the Bank's EDR/XDR, SIEM and threat-intelligence platforms. The solution shall support ingestion of external threat-intelligence to enrich and prioritise workload findings."	No Change, Please be guided by the RFP
1971	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 47 and S.No. 48	S.No. 47 - The solution shall support high availability and service continuity appropriate to the proposed deployment architecture and shall provide mechanisms for recovery of relevant configurations and security policies. S.No. 48 - The solution shall provide mechanisms to identify the protection health/status of onboarded workloads, including agent, connector or communication health where applicable.	For OEM-managed SaaS delivery, high availability, redundancy and disaster recovery are provided within the OEM platform under its published availability SLA and cannot be operated or restored by the Bank. We request you to kindly update S.No. 47 as following - "For SaaS-delivered solutions, the OEM shall provide high availability, redundancy and disaster recovery within the platform in line with its published availability SLA and shall provide mechanisms for export/retrieval of relevant configurations and security policies. For on-premises components, if any, the solution shall support HA and documented backup-restore." For S.No. 48, we request confirmation that reporting of connector/cloud-account onboarding and assessment health (and agent health only where an agent is proposed) shall be treated as compliant.	Please refer addendum for revised clause S.No. 47 - The solution shall support service continuity appropriate to the proposed deployment architecture and shall provide mechanisms for recovery of relevant configurations and security policies. Clarification S.No. 48 - Bidder to propose the aproach ensuring the compliance with the sought requirement. Reporting of connector/cloud-account onboarding and assessment health shall also be considered compliant. Agent health reporting shall apply only where an agent is proposed/deployed.
1972	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 49	The solution shall support consumption and correlation of relevant vulnerability, SBOM, CBOM and threat-intelligence information from the Bank's separately procured security solutions through APIs, supported integrations or equivalent mechanisms, where technically supported.	Consumption of Cryptographic Bill of Materials (CBOM) is an emerging requirement with no single established interchange standard, and correlation is only feasible if the source system and format are known. We request you to kindly confirm (a) the source solutions and the exact formats/standards in which SBOM and CBOM will be provided by the Bank (e.g., CycloneDX, SPDX and version), and (b) that where a standard format/API is not made available by the source solution, non-availability of such correlation shall not be treated as non-compliance, consistent with the qualifier 'where technically supported' in the clause.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1973	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM - Section scope (S.No. 1 to 69 and TOTAL MARKS 690)	Continuous Threat Exposure Management (CTEM) - all functional specifications, S.No. 1 to 69, TOTAL MARKS 690.	A significant proportion of the CTEM section (illustratively S.No. 1, 2, 5, 7 to 13, 18 to 23, 35, 55, 56, 57 and 67) specifies Cyber Threat Intelligence (CTI) and Digital Risk Protection (DRP) service deliverables - multilingual dark-web collection and translation, analyst-authored periodic and ad-hoc research reports, VIP investigation reports, threat-actor dossiers and engagement with threat actors, compromised-credential and payment-card monitoring, takedown/reporting to external authorities, named analyst and incident-response services. These are analyst-delivered managed services and are distinct from a Continuous Threat Exposure Management platform, which (per the recognised CTEM framework) delivers scoping, discovery, prioritisation, validation and mobilisation of exposures across the attack surface. As currently drafted, the section can be fully met only by DRP/CTI service providers and is restrictive to exposure-management platform OEMs, even though the Bank has separately (at VA-VM S.No. 87 and 88) contemplated CTEM as the platform that consolidates and prioritises findings across scanning engines. We therefore request you to kindly split this section into (a) 'CTEM / Exposure Management Platform' and (b) 'Cyber Threat Intelligence and Digital Risk Protection Services', with separate functional specifications, separate marks and separate	No Change, Please be guided by the RFP
1974	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 1, S.No. 2 and S.No. 7	S.No. 1 - The solution should collect intelligence from multiple languages and relevant regional sources, with support for multilingual threat intelligence processing and analysis. S.No. 2 - The solution should support translation or interpretation of collected intelligence into English. S.No. 7 - Each intelligence item should include metadata such as date, author, source, and pre-classification of raw data.	Multilingual collection from closed/regional sources, machine translation of collected raw intelligence, and 'author'-level metadata with pre-classification of raw data are characteristics of a dark-web/DRP collection platform and are not features of a CTEM/exposure management platform. We request you to kindly move these clauses to the proposed Cyber Threat Intelligence/DRP service scope. If they are retained under CTEM, we request you to kindly update them as following - "The solution shall provide vulnerability, exploit and exposure intelligence in English, with source, publication date and classification metadata, and shall support ingestion of multilingual/regional intelligence from bank-approved third-party sources through supported integration mechanisms."	Please refer the addendum for revised clause
1975	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 8 and S.No. 53	S.No. 8 - The solution should allow messaging and collaboration within the context of a specific intelligence item. S.No. 53 - Each alert should include a discussion board for eligible users to collaborate within the alert context.	An in-product messaging/discussion board is a vendor-specific user-interface feature, and for a bank, collaboration and audit trails on security findings are better retained in the Bank's ITSM/SOAR system of record rather than in a third-party SaaS console. We request you to kindly update the clauses as following - "The solution shall support collaboration on a specific exposure, alert or intelligence item through comments/annotations, assignment and status tracking within the platform and/or through bidirectional integration with the Bank's ITSM/SOAR/ticketing platform."	No Change, Please be guided by the RFP
1976	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 9	The solution shall provide access to proprietary, internally generated, licensed or equivalent high-quality threat intelligence sources capable of providing actionable intelligence relevant to the Bank's environment.	We request confirmation of the nature of intelligence expected. Exposure-management OEMs provide proprietary research-generated vulnerability, exploit and exposure intelligence (including exploit availability, exploitation-in-the-wild, ransomware association and predictive exploitability), whereas dark-web/actor intelligence is sourced by DRP providers. We request you to kindly update the clause as following - "The solution shall provide access to the OEM's proprietary/internally generated and/or licensed intelligence covering vulnerabilities, exploits, exploitation activity and exposures relevant to the Bank's environment, and shall support ingestion of additional bank-approved third-party intelligence sources."	No Change, Please be guided by the RFP
1977	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 10	Analysts should perform threat hunting activities to find findings outside of the platform.	This clause requires a human analyst-delivered managed service and is not a functional specification of a solution. Scoring it within a functional compliance sheet at 10 marks does not permit objective evaluation. We request you to kindly move this clause to the managed services/MSSP or CTI service scope of the RFP with defined service levels (number of analyst hours, hunting frequency, deliverable and reporting format) and a separate commercial line item, so that bidders can price it objectively. If it is retained, kindly define the expected analyst effort and deliverables.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1978	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 11	The solution/service should generate investigation reports for designated VIPs or other high-risk identities/assets, providing an overview of identified digital exposure and associated risk.	VIP/executive digital exposure investigation is a Digital Risk Protection service deliverable involving collection of personal digital footprint data, and carries data-protection considerations under the DPDP Act for the named individuals. We request you to kindly move this clause to the Cyber Threat Intelligence/DRP service scope. If retained, kindly confirm the number of designated VIPs/high-risk identities, the frequency of such reports and the consent/lawful-basis framework the Bank will provide for processing their personal data, so that bidders can price and lawfully deliver the service.	No Change, Please be guided by the RFP
1979	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 5, S.No. 12 and S.No. 13	S.No. 5 - automated and/or AI-assisted generation of tailored intelligence reports based on customer requirements. S.No. 12 - general and industry-related cyber intelligence reports on threat landscape trends, at least twice a month. S.No. 13 - the solution should be able to commission ad-hoc research reports on demand.	Periodic (twice monthly) industry threat-landscape reports and ad-hoc commissioned research reports are analyst-authored service deliverables, and 'on demand' without a defined ceiling is commercially open-ended. We request you to kindly move these clauses to the Cyber Threat Intelligence service scope with defined deliverables, and kindly confirm (a) the maximum number of ad-hoc research reports that may be commissioned per annum, (b) the expected turnaround time, and (c) whether these are to be priced within the platform subscription or as a separate service line item.	a. Periodic industry threat-landscape reports - At least a month b. Ad-hoc commissioned research reports: The requirement shall shall relate to threats, exposures, vulnerabilities and risk areas relevant to the Bank c. Bidder to ensure that all requite cost is factored and the requirement is complied at not additional to the bank Please refer addendum for revised clause
1980	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 18	The solution should provide comprehensive threat actor attribution including known identities, motivations, historical activity, TTPs, associated infrastructure, and MITRE ATT&CK mapping.	Threat-actor attribution dossiers covering actor identities, motivations and associated infrastructure are CTI/DRP deliverables. Exposure-management platforms provide threat-actor and campaign context mapped to MITRE ATT&CK for the vulnerabilities and exposures identified in the Bank's environment. We request you to kindly move this clause to the Cyber Threat Intelligence service scope, or update it as following - "The solution shall provide threat context for identified exposures, including associated threat actors/campaigns, observed exploitation activity, TTPs and MITRE ATT&CK mapping, where such intelligence is available, and shall support enrichment from bank-approved third-party threat-intelligence sources."	Please refer addendum for revised clause
1981	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 19	The solution should detect compromised credentials for employees and VIPs, exposed payment card information, and aggregate data from known breach databases in real time	Detection of compromised credentials and exposed payment-card data through aggregation of breach and dark-web databases is a Digital Risk Protection capability and requires the provider to collect, store and process the Bank's employees' and customers' personal and card data, with attendant DPDP Act and PCI DSS implications. We request you to kindly move this clause to the Cyber Threat Intelligence/DRP service scope of the RFP. If retained under CTEM, kindly confirm the employee/identity count and card-BIN ranges to be monitored, and the data-processing and retention framework the Bank will mandate for such personal and cardholder data.	Please refer addendum for revised clause
1982	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 21	The solution should support threat actor interaction via vendor analysts (e.g., engaging via dark web avatars) to gather additional intelligence	Engagement with threat actors through covert dark-web personas is offered by a very small number of DRP providers, cannot be objectively evidenced or evaluated in a technical compliance sheet, and exposes a regulated bank to legal, reputational and regulatory risk arising from interaction with criminal actors on its behalf. We request you to kindly remove this clause from the CTEM functional specifications, as it is restrictive to a limited set of vendors and is not required to achieve continuous threat exposure management outcomes. If the Bank wishes to retain such capability, we request it be moved to an optional service line item, excluded from the technical scoring.	Please refer addendum for the revised clause Clause Stands deleted
1983	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 23	The solution should support reporting of confirmed malicious or phishing assets to relevant external platforms and authorities, where such reporting is supported and authorized.	Reporting and takedown of malicious/phishing domains and assets with registrars, hosting providers, app stores and authorities is an anti-phishing/brand-protection service, delivered under authorisation letters from the brand owner. We request you to kindly move this clause to the anti-phishing/brand protection service scope. If retained, kindly confirm the expected number of takedown/reporting requests per annum and the applicable turnaround SLA, and confirm that the Bank will provide the requisite authorisation to act on its behalf, so that bidders can price the service.	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1984	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 20, 22, 45 and 47	S.No. 20 - IoC enrichment allowing submission of IPs, domains and hashes to receive contextual threat intelligence and threat actor attribution; S.No. 22 - scanning and reputation analysis of submitted IP addresses; S.No. 45 - manual IoC management operations; S.No. 47 - cross-platform IoC enforcement across the security stack.	IoC submission, enrichment, lifecycle management and - in particular - enforcement of IoCs across the security stack are functions of a Threat Intelligence Platform (TIP) and SOAR, both of which are in scope of this RFP. Enforcement (pushing blocklists to NGFW, proxy, DNS, EDR and email gateways) is performed by those controls under the Bank's change-management process, not by an exposure-management platform. We request you to kindly move S.No. 45 and S.No. 47 to the TIP/SOAR scope, and update S.No. 20 and S.No. 22 as following - "The solution shall support enrichment of submitted indicators (IP addresses, domains, hashes) with available contextual intelligence and reputation information natively and/or through integration with the Bank's threat-intelligence platform, and shall support publishing of validated indicators to the Bank's security controls through the Bank's SOAR/TIP."	Please refer addendum for the revised clause
1985	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 24	The solution should provide pre-built bidirectional integrations with SIEM, SOAR, ticketing (Manage Engine), and threat intelligence platforms	Availability of a 'pre-built' connector is vendor-specific, whereas equivalent bidirectional integration is routinely achieved through documented REST APIs and webhooks with the same functional outcome. We request you to kindly share the Vendor/Model/Version of the SIEM, SOAR, ManageEngine ticketing product and threat-intelligence platform to be integrated, and update the clause as following - "The solution shall provide bidirectional integration with the Bank's SIEM, SOAR, ticketing (ManageEngine) and threat-intelligence platforms through pre-built connectors, documented REST APIs, webhooks or equivalent mechanisms."	Please refer addendum for the revised clause
1986	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 30 and S.No. 33	S.No. 30 - The solution shall provide automated validation of identified exposures, where technically applicable and authorized by the Bank, using controlled, non-destructive testing or equivalent validation mechanisms to determine whether the identified exposure is genuinely exploitable or materially exposed. S.No. 33 - The solution should validate that a vulnerability is actually exploitable or otherwise materially exposed (active exposure validation).	Active, automated exploitation-based validation of findings is the function of Breach and Attack Simulation (BAS) or automated penetration-testing tooling - which the Bank itself references at S.No. 41 of this section as a separate external source to be integrated. Exposure-management platforms establish material exposure and exploitability through evidence-based validation: authenticated/unauthenticated verification of the finding, reachability and internet-exposure analysis, attack-path analysis, exploit availability and exploitation-in-the-wild intelligence. We request you to kindly update the clauses as following - "The solution shall validate whether an identified exposure is genuinely exploitable or materially exposed using evidence-based validation - including verification of the finding, internet exposure and network reachability analysis, attack-path analysis, exploit availability and observed exploitation intelligence - and shall support ingestion of validation results from the Bank's BAS/penetration-testing tools through supported integration." Kindly also confirm that active exploitation testing against the Bank's production environment is not mandated as a day #1 platform capability.	Please refer addendum for the revised clause
1987	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 35	The solution should detect malicious files, reconnaissance activity, automated attack tools, and target lists	Detection of reconnaissance activity, automated attack tooling and 'target lists' naming the Bank requires deception/honeypot sensors, network detection telemetry or dark-web collection, none of which are capabilities of a CTEM/exposure management platform. We request you to kindly remove this clause from the CTEM section (reconnaissance and attack-tool detection being already addressed by the Bank's NDR, WAF, NGFW and SOC/SIEM scope), or move it to the Cyber Threat Intelligence/DRP service scope.	Please refer addendum for revised clause
1988	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 41	The solution should support external vulnerability source integrations such as VA/VM scanners, ASM, XDR, BAS, Dark Web Monitoring, and MDM/UEM	Integration is feasible only where the source product, version and API are known, and Dark Web Monitoring and BAS are separate product categories which the Bank may or may not have licensed. We request you to kindly (a) share the Vendor/Model/Version of each source solution to be integrated (VA/VM, ASM, XDR, BAS, Dark Web Monitoring, MDM/UEM), (b) confirm which of these the Bank already owns and which are expected to be supplied by the bidder, and (c) confirm that non-availability of integration with a product the Bank has not licensed, or which does not expose a supported API, shall not be treated as non-compliance.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1989	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 42 and S.No. 43	S.No. 42 - The solution should use machine learning to evaluate the business impact of each remediation action and prioritize high-priority exposures. S.No. 43 - The ML model should continuously study the environment including asset relationships, topology, and security controls to detect false positives and identify root causes.	These clauses mandate a specific implementation mechanism ('machine learning', 'the ML model') and a specific analytic behaviour rather than the security outcome, which is restrictive to a particular OEM's product design. The Bank has adopted a technology-neutral formulation elsewhere in this very section (S.No. 34 - 'using AI/ML or equivalent analytic'). We request you to kindly update the clauses as following, consistent with S.No. 34 - "The solution shall prioritise exposures using AI/ML or equivalent analytics based on asset criticality and business context, exploitability, exposure, asset relationships/topology and the effect of existing security controls, and shall support identification of false positives and of common root causes to enable efficient remediation."	No Change, Please be guided by the RFP
1990	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 38 read with S.No. 41 and S.No. 48	S.No. 38 - The solution should be deployed agentlessly, without requiring sensors or agents on endpoints, servers, or network appliances. S.No. 41 - external vulnerability source integrations such as VA/VM scanners, ASM, XDR, BAS, Dark Web Monitoring, and MDM/UEM. S.No. 48 - The solution should assess and harden network, endpoint, and operating system security controls.	S.No. 38 mandates a fully agentless and sensor-less deployment, while S.No. 48 requires assessment and hardening of endpoint and operating-system security controls - which requires either a credentialed/authenticated scan, an agent, or ingestion from the agent-based VA/VM, XDR and MDM/UEM platforms referenced in S.No. 41. These clauses partially contradict each other. We request you to kindly confirm that the CTEM platform itself may remain agentless and derive endpoint/OS control assessment through integration with the Bank's VA/VM, XDR and MDM/UEM platforms and credentialed configuration audit performed by those tools, and kindly update S.No. 48 as following - "The solution shall consolidate and report on the configuration/hardening posture of network, endpoint and operating system security controls, natively and/or by ingesting configuration and compliance assessment results from the Bank's VA/VM, XDR, MDM/UEM and related platforms."	Please refer addendum for the revised clause
1991	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 49 and S.No. 50	S.No. 49 - The solution should provide a private exposure map of the organization's attack surface. S.No. 50 - The solution should support custom protections tailored to the organization's environment.	The terms 'private exposure map' and 'custom protections' are vendor-specific product terminology and are not objectively evaluable; 'protections' further implies enforcement, which a CTEM platform does not perform. We request you to kindly update the clauses as following - S.No. 49 - "The solution shall provide a consolidated, access-controlled map/inventory of the organisation's internal and internet-facing attack surface, including assets, relationships, exposures and attack paths." S.No. 50 - "The solution shall support custom policies, custom detection/assessment rules, custom risk scoring and custom tagging tailored to the organisation's environment."	S.No 49.: Please refer addendum for revised clause Clarification: S.No 50: " & M500
1992	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 51, 59, 60, 62 and 63	S.No. 51 - apply virtual patching/compensating controls/exposure mitigation mechanism to the firewall and other security systems through integration with relevant security controls; S.No. 59 - API-based remediation, notification or workflow integration with relevant security controls; S.No. 60 - automated remediation workflows; S.No. 62 - leverage compensating controls and layered defense strategies; S.No. 63 - collaboration tools and ITSM integration for remediation workflows.	These clauses require the CTEM platform to execute configuration changes directly on the Bank's production security controls (firewall, WAF, IPS, EDR). In a regulated banking environment such changes must pass through the Bank's change-management and maker-checker controls, and the accountable system of record for orchestration is the Bank's SOAR/ITSM, which is separately in scope under this RFP. We request you to kindly update the clauses as following - "The solution shall identify applicable compensating controls, virtual patching and exposure-mitigation options for identified exposures, shall provide the corresponding remediation/mitigation instructions and artefacts, and shall trigger and track remediation through API/webhook-based integration with the Bank's SOAR, ITSM and relevant security controls. Actual enforcement of changes on production security controls shall be performed by the respective control through the Bank's approved change-management process." Kindly confirm that compliance achieved through such SOAR/ITSM-orchestrated remediation shall not be treated as non-compliance.	Please refer addendum for revised clause Clarification: S.No 63: No Change, Please be guided by the RFP.
1993	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 61	The solution should ensure remediation actions do not disrupt business continuity	A security platform can assess and present the potential impact of a recommended remediation, but it cannot guarantee the business-continuity outcome of a change executed on the Bank's production systems, which depends on the Bank's change-management, testing and rollback processes and on the affected application's architecture. As worded, the clause places an unqualified guarantee on the bidder/OEM. We request you to kindly update the clause as following - "The solution shall provide impact assessment and risk context for recommended remediation actions, including affected assets, dependencies, prerequisites and rollback considerations, to enable the Bank to plan and execute remediation without disrupting business continuity through its change-management process."	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
1994	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 55 and S.No. 56	S.No. 55 - The solution should include IOC investigation, infrastructure mapping, and threat actor identification. S.No. 56 - The visual investigation tool should integrate multiple services including WHO IS and Passive DNS.	A graph-based 'visual investigation tool' bundling WHOIS, Passive DNS and threat-actor identification is a specific feature of certain CTI/DRP investigation products and is not a CTEM platform capability; it is also available to the Bank through its threat-intelligence platform in scope under this RFP. We request you to kindly move these clauses to the Cyber Threat Intelligence/DRP or TIP scope, or update them as following - "The solution shall support investigation of identified exposures and indicators, including mapping of the Bank's internet-facing infrastructure and associated relationships (such as domains, sub-domains, certificates, DNS and WHOIS/registration data for the Bank's own digital footprint), and shall support enrichment and threat-actor context through integration with the Bank's threat-intelligence platform."	No Change, Please be guided by the RFP
1995	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 57, S.No. 58 and S.No. 67	S.No. 57 - Up on demand, the vendor should provide a dedicated Customer Success Manager as a single point of contact for onboarding and ongoing support. S.No. 58 - The vendor to provide 24/7 system support. S.No. 67 - The vendor to provide a mechanism to report security incidents identified through the platform and receive prompt response and guidance from the incident response team.	These are commercial/service clauses rather than functional specifications of the solution, and 'dedicated Customer Success Manager' and access to an 'incident response team' are named-resource and incident-response-retainer commitments that cannot be objectively evaluated in a functional compliance sheet or priced without defined limits. We request you to kindly move these clauses to the services/SLA section of the RFP and confirm - (a) whether the Customer Success Manager is required to be dedicated to the Bank full-time or is an assigned named point of contact, and whether onsite presence is expected; (b) the required support SLA and severity-wise response/resolution matrix for 24/7 support; and (c) for S.No. 67, the number of incident-response engagements per annum, whether remote or onsite, and whether these are to be priced within the subscription or as a separate retainer.	No Change, Please be guided by the RFP
1996	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 65 and S.No. 66	S.No. 65 - The solution should aim to reduce Mean Time to Remediate (MTTR) and labor costs. S.No. 66 - The solution should maximize ROI from existing security tools by optimizing the security posture.	These clauses express desired business outcomes rather than verifiable functional specifications, and each carries 10 marks in a scored technical compliance sheet. Compliance cannot be objectively demonstrated or evaluated, and every bidder will necessarily mark itself compliant, which adds no discriminatory value to the Bank's evaluation. We request you to kindly either remove these clauses from the scored functional specifications, or replace them with measurable requirements as following - S.No. 65 - "The solution shall provide MTTR measurement and trending for exposures by severity, asset criticality and business unit, including SLA tracking and ageing analysis." S.No. 66 - "The solution shall provide coverage and control-effectiveness reporting across the Bank's existing security tools, identifying assets not covered by, or gaps in, existing security controls."	Please refer addendum for revised clause
1997	49	7.3.11 Cloud Security (CSPM) Tool		7.3.11 (Preamble) - Integrated cloud security solution providing a centralized and unified single-pane-of-glass view across all cloud assets, workloads, identities, configurations, applications, containers, AI services and cloud-native resources deployed across multi-cloud, hybrid-cloud and on-premises environments.	Unified visibility across cloud assets, workloads, identities, configurations, containers, Kubernetes, AI services and cloud-native resources across multi-cloud and hybrid-cloud is met from a single console. Deviation: 'on-premises environments' - CSPM assesses cloud provider control planes through APIs and has no control plane to assess for traditional on-premises infrastructure. On-premises posture is delivered through configuration/compliance benchmark auditing in the VA & VLM solution, and on-premises Kubernetes through the cloud security platform. Request the Bank confirm that on-premises security posture assessed via CIS/benchmark configuration audit in the VA & VLM solution, consolidated into the same single pane, is acceptable.	No Change, Please be guided by the RFP
1998	50	7.3.11 Cloud Security (CSPM) Tool		7.3.11.2 (10) - Key Deliverable: Incident Response & Automated Playbooks.	The platform provides prioritized findings, remediation guidance, auto-generated remediation code (IaC/CLI), and event/webhook/API triggers that drive downstream automation. Deviation: incident response playbook authoring and execution is SOAR functionality, and SOAR is separately in scope under this RFP. The CSPM tool cannot itself be the playbook execution engine. Request the Bank confirm that this deliverable will be met by publishing CSPM findings and triggers into the Bank's SOAR/ITSM, with the response playbooks built and executed there.	No Change, Please be guided by the RFP
1999	51	7.3.11 Cloud Security (CSPM) Tool		7.3.11.2 (12) - Ensure that the reports are extracted from online / warehouse storage etc. Restore the logs/data from backup for forensic investigation and as per bank requirement without any additional cost.	Findings, assessment history, audit logs and reports are retrievable on demand through the console, scheduled reports and APIs at no additional cost for the retention period applicable to the subscription. Deviation: for an OEM-managed SaaS platform there is no Bank-accessible backup media from which data is 'restored'; data is served from the live platform and its retention tier. Request the Bank (a) specify the mandated retention period, and (b) accept on-demand retrieval/export from the platform as fulfilling this requirement.	Please refer the addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2000	29	7.2.1	Security Information and Event Management (SIEM)	Bank Location: Broker/Aggregator/Collector: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Cloud (SaaS): HA Deployment aligned with the SLA, RTO & RPO (Refer Section 13). Management Console: Deployed at both Primary and Secondary sites	In the RFP, there is an ask for management console deployment across DC-DR. If the bidder is offering SAAS platform can this requirement be relaxed.	No Change, Please be guided by the RFP
2001	37	2	For SIEM Solution	Primary Log Storage & Retention (Raw SIEM logs shall be retained on the Cloud-designated primary storage for a minimum period of 1 month in their original/unmodified form, along with relevant timestamps, source information and metadata. Parsed, normalized, enriched, indexed and correlated logs, together with associated metadata and contextual information, shall be retained for a minimum period of 60 months (5 years).)	To meet this requirement can the OEM store the same in their cloud or is it expected to have the log storage done in Banks premises.	No Change, Please be guided by the RFP
2002	57	7.4.6	Dark Web Monitoring	The Bidder shall provide offsite, tool-based continuous dark web and cyber threat exposure monitoring services to identify potential exposure of the Bank's sensitive information across the surface web, deep web, dark web, underground forums, messaging platforms, and data leak repositories.	For the darkweb monitoring can you help with the domains to be considered and no of takedowns to consider in the proposal	Detailed domain and identity information shall be provided to the selected bidder on a need-to-know basis
2003	64	7.6.6	Testing- Activities are to be performed by Respective solution OEM (supported by bidder)	The bidder shall provision and maintain dedicated Development, Testing, UAT, and Pre-Production environments throughout the contract period. All software, licenses, and other resources required for such environments shall be included within the bidder's scope without any additional cost to the Bank.	Can this be hosted in the OEM's cloud or is it required to be hosted in banks premises?	No Change, Please be guided by the RFP
2004	68	7.7	The proposed Cloud/SaaS solution shall support Bring Your Own Key (BYOK) and/or Customer-Managed Encryption Key (CMEK) capability, enabling the Bank to maintain control over the cryptographic keys used to protect its security data		Can this clause be relaxed or read as dedicated key for the customer to be provisioned with customer security policies enforced for the same?	No Change, Please be guided by the RFP
2005	73	7.12.3	2 OEM Implementation Resources	Onsite (Full Time) OEM shall submit a detailed resource deployment plan commencement of requirement gathering. Any replacement or modification shall require prior Bank approval.	Can this clause be relaxed or read as OEM resources to be available during the deployment phase only and be made available when needed?	No Change, Please be guided by the RFP
2006		Decoy Functional Requirements: Point 9		Deployment capability:- • Should support Central Management for distributed Deployment. • Should support extension of Decoy from a central location to remote offices/location or cloud infrastructure. • Should support auto VLAN detection and addition to deployment networks. • Should support command line based approach for Decoy deployment	The solution supports all the points mentioned. However we humbly request to modify the clause "Should support command line based approach for Decoy deployment" to "Should support autonomous deploymrents for Deceptions that is triggered from a gui-based console or using APIs" Justification: To manage a large deception deployment, deception deployment through a command line interface makes it operationally complex to manage and prone to operator errors. The deception solution for a large bank like PSB is required to support autonomous deployment with very little operator involvement to guarantee ease of deployment. If the CLI based interface is required for automation, recommend that an API based interface (besides gui based) be given as an option.	No Change, Please be guided by the RFP
2007		Decoy Functional Requirements: Point 19		The deception module generates actionable threat intelligence based on decoy interactions, with insights on attacker behaviors like botnet activity, frequent attacks, security scanner usage, and other IP attributes. Includes real-time traffic patterns (hourly, weekly, monthly) and detailed attack types (region-wise, ISP-wise, decoy-wise).	Please clarify if this requirement is for Internet facing Deceptions. The reason for this question is because there is a requirement for a region, ISP wise breakup. This would not be relevant for Decoys deployed within the enterprise.	No Change, Please be guided by the RFP
2008		Decoy Functional Requirements: Point 20		Includes an algorithm for automated rule creation that integrates with SOAR platforms, enabling real-time blocking of attacker IPs based on threat intelligence gathered from decoys. Features a customizable Generative AI model to assist security analysts with contextual insights, investigative support, and proactive security measures.	The solution includes a AI module that automatically triages and corelates deception observations to generate a high-fidelity deception incident. Respectfully request that the specific technique for AI (Generative AI based model) be ommitted from the requirement and reword the requirement to "Features a customizable AI module to assist security analysts with contextual insights, investigative support, and proactive security measures."	Please refer addendum for revised clause.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2009		Decoy Functional Requirements: Point 21		Captures commands executed on high-interaction decoys with minimal performance impact, using agentless/agent mechanisms. Decoys feature self-deletion and self-triggering to remain undetected by attackers.	The solution does capture commands executed on high-interaction decoys without impacting production workloads. Humbly request that the "Decoys feature self-deletion and self-triggering to remain undetected by attackers." requirement be reworded to "Deceptions should not be fingerprintable by an attacker" Justification: Depending on the detection usecase, Self-Deletion could be used by adversarties to fingerprint deceptions. Hence, the overall objective of not being fingerprintable should be kept as the requirement, the specific mechanisms to achieve it can change based on the solution and usecase.	No Change, Please be guided by the RFP
2010		Decoy Functional Requirements: Point 22		Offers Malware Analysis for malware captured via decoys or externally submitted samples. Includes static and dynamic analysis, reverse engineering, and behavior monitoring in a secure sandbox. Detailed reports include IOCs, persistence mechanisms, and containment recommendations.	The solution does capture malware executed in the deception environment for malware analysis. The solution does not support malware analysis for externally submitted samples Request that the clause "or externally submitted samples" be ommitted as that is not a Deception functionality.	No Change, Please be guided by the RFP
2011		Decoy Functional Requirements: Point 23		The proposed solution shall provide an deception technology platform capable of deploying agentless and/or agent-based deception techniques to detect, delay, and identify unauthorized access, lateral movement, reconnaissance, credential theft, and malicious activities by presenting deceptive assets, services, credentials, and attack paths across the enterprise environment.	The RFP requires breadcrumbs to be deployed on 12000 endpoints. Putting another privileged deception endpoint agent on each of those 12000 endpoints increases the attack surface across the entire network including the huge risk of privilege escalation and supply-chain attacks. Request to change this requirement to agentless deception techniques. This will also avoid all resource usage issues on production endpoints.	No Change, Please be guided by the RFP
2012		Decoy Functional Requirements: Point 25		"The proposed solution shall be delivered as a cloud-based/SaaS platform hosted within the CSP environment. The bidder shall provision and size the required cloud compute, storage, network, and other platform resources to meet the Bank's performance, scalability, High Availability (HA), service continuity, and Disaster Recovery (DR) requirements in accordance with the applicable Cloud Deployment Model."	Please confirm that the solution can be offered as a SaaS service	Please refer addendum for revised clause.
2013	Page No: 259	Volumetrics- Solution-wise Requirements: Point 8		Proposed Solution must cover complete scope of min of 200 applications, networks, devices with 50 segments across DC-DR and capability to add additional decoy connector through decoy customization as per requirement of PSB.	The RFP specifies a minimum requirement of 200 decoys. Since breadcrumbs will be deployed across 12,000+ endpoints, we recommend increasing the decoy count beyond the specified minimum to ensure better distribution of breadcrumbs and reduce the possibility of fingerprinting. We respectfully recommend that the minimum decoy count be amended to 600 decoys."	Please refer addendum for revised clause.
2014					Request to add additional OEM eligibility criteria to ensure deployment success: 1) Given there are 12000 endpoints it seems appropriate to have an elgibility criteria for deception tech OEM to have alteast deployed 500+ decoys in a single deployment in India and 1000+ globally. Hence humbly request that the single bank deployment criteria is enhanced to specifiy atleast 500+ deceptions should have been deployed. 2) To demonstrate successful deployment experience, we request that the OEM share atleast 3 POs for deception deployments, that have been operational for at least one year. This will help establish successful implementation. 3) To demonstrate Market Leadership, request that a criteria be added that the OEM must be tracked and rated as a leader by one or more global analysts like Gartner, KuppingerCole or GigaOM.	No Change, Please be guided by the RFP
2015	95	Dark Web Monitoring	Web Logs		Dark Web Monitoring solutions are designed to scan external sources on dark web rather than parse private network traffic or server logs.	Please refer addendum for revised clause.
2016	95	Dark Web Monitoring	Payment Intelligence		Need More Context	No Change, Please be guided by the RFP
2017	47	SLA Queries (SOW, Page 47)			Phishing URL Takedown: We request that the site takedown resolution time for identified phishing URLs be adjusted to a minimum of 48 hours (instead of 24 hours).	No Change, Please be guided by the RFP
2018	47	SLA Queries (SOW, Page 47)			Brand Abuse Takedown: We request that the site takedown resolution time for brand abuse be adjusted to a minimum of 48 hours (instead of 36 hours).	No Change, Please be guided by the RFP
2019	47	Penalty Query (SOW, Page 47)			We kindly request that the bank revise the penalty clause to cap penalties per technology at 10% of that specific technology's contract value, rather than the overall contract value.	No Change, Please be guided by the RFP RFP Clause 13.2 - For the purpose of this RFP, the total penalties as per LD & SLA will be subject to a maximum of 10% of the overall contract value
2020	117	10.2	Eligibility Criteria-Clause-22	The proposed OEM solution should have been implemented in at least one verifiable client in India. Credential is to be submitted for the following solutions: a. CNAPP b. CWPP c. CTEM	CTEM is a new framework and customers are still in evaluation/ Implementation phase. Suggested change Client in India or Global BFSI The proposed OEM solution should have been implemented in verifiable client in India or Global. Credential is to be submitted for each of the following solutions: 1. CNAPP 2. CWPP 3. CTEM	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2021	120	10.2	Eligibility Criteria-Clause-23	The proposed OEM services should have been implemented in at least one (1) PSU/ PSE/ Government Organizations / BFSI in India. Credential is to be submitted for the following services: 1. Breach Attack & Simulation 2. Continuous Automated Red Teaming 3. Attack surface management 4. Phishing simulation 5. Anti-phishing services 6. Dark web monitoring 7. Brand protection & monitoring 8. Threat Intelligence feed 9. Threat Hunting services	As the offsite services are specified under the functional compliance requirements and are expected to be provided by the bidder, the corresponding eligibility criteria should be assessed at the bidder level. Suggested Changes: The proposed bidder services (below mentioned to the services) should have been implemented by the bidder in in at least one verifiable client in India.	No Change, Please be guided by the RFP
2022	86	16	Technical Specs-Anti Phishing-	Solution must be able to seamlessly integrate with On-Prem Mail Gateways via Mail Transfer Agent (MTA) forwarding	Anti-Phishing is asked as a Managed service however MTA is a componentfor onprim SEG gateway Suggested Change: Solution must be able to seamlessly integrate with On-Prem Mail Gateways via API integration	Please refer to the relevant Addendum for updated specfications
2023	87	18.2	Technical Specs-Anti Phishing-	Solution must provide DoS protection and directory harvest attack protection to ensure the availability of email services	DOS Protection Is Typically the Responsibility of the hardware based Email Infrastructure or Secure Email Gateway or Firewall or dedicated DDOS protection Hence this clause should not fall under Anti-Phishing services Also, this feature Suggested Change: Remove this clause	Please refer to the relevant Addendum for updated specfications
2024	87	19.2	Technical Specs-Anti Phishing	Solution must be able to display HTML banners on email clients, automatically switching to plain text format if HTML is not supported, while also providing multilingual support based on the organization's language preferences. HTML banner content can be edited or customized by organization	The requirement appears to prescribe a specific notification mechanism (HTML banner insertion) rather than the intended security outcome of user awareness and phishing risk notification. Modern anti-phishing solutions may provide user alerts through native email client warnings, subject tagging, security indicators, API-based notifications, or other mechanisms without relying on HTML banner injection. Suggested Change: Remove the clause	Please refer to the relevant Addendum for updated specfications
2025	87	19.4	Technical Specs-Anti Phishing	Solution must offer multiple disposition options, including attachment stripping, delivery of notices to senders, and quarantine of the whole email	Delivery of notice is platform specific feature Suggested Change Solution must offer multiple disposition options, including attachment stripping, and quarantine of the whole email	Please refer to the relevant Addendum for updated specfications
2026	87	19.5	Technical Specs-Anti Phishing	Solution must provide a "Safe Preview" capability for administrators to view detailed information of quarantined messages and decide necessary actions	Safe Preview is a broad term, it should relate to anti-phishing Suggested Change Solution must provide a "Safe Preview of links" capability for administrators to view detailed information of quarantined messages and decide necessary actions	Please refer to the relevant Addendum for updated specfications
2027	88	19.8	Technical Specs-Anti Phishing-	As part of the forensic collection, should include the capture of PowerShell history	The requirement appears to mandate a specific forensic artefact (PowerShell history) rather than the intended security objective of investigating PowerShell-based activity. Suggested Change As part of the forensic collection, should include the capture of PowerShell history or equivalent forensic mechanism	Please refer to the relevant Addendum for updated specfications
2028	88	19.17	Technical Specs-Anti Phishing-	Solution must provide detailed reporting covering system usage and other areas including global message summary, spam, virus and other rule actions to save administrator time and effort in the collection of data for status reports. Reports can be emailed (HTML), printed, or downloaded in CSV format for use with third party tools	Suggested Changes: Solution must provide detailed reporting covering system usage and other areas including global message summary, spam, virus and other rule actions to save administrator time and effort in the collection of data for status reports. Reports can be emailed (HTML), printed, or downloaded in CSV or PDF format for use with third party tools	Please refer to the relevant Addendum for updated specfications
2029	88	19.18	Technical Specs-Anti Phishing-	Solution must have capability for administrators to view reports containing detailed statistics covering emails processed, rejected emails, SMTP transactions, and communication flows	The requirement mandates visibility into SMTP transactions and communication flow analytics, which are traditionally functions of MTA,and may not have direct access in API-based or cloud-native anti-phishing solutions. Suggested Change Solution must have capability for administrators to view reports containing detailed statistics covering emails processed, rejected emails.	Please refer to the relevant Addendum for updated specfications
2030	89	19.37	Technical Specs-Anti Phishing-	Solution must support message classification management, including separate classifiers for spam, impersonation, bulk, phishing, adult, and malware messages, with the ability to set score thresholds per category.	The requirement mandates a specific detection architecture based on separate classifiers and per-category scoring thresholds. Modern email security and anti-phishing solutions increasingly leverage AI/ML models, behavioural analytics, graph intelligence, and composite risk engines that may not expose individual classifiers Suggested Change Solution must support message classification management, including separate classifiers for spam, impersonation, bulk, phishing and malware messages, with the ability to set score thresholds per category.	Please refer to the relevant Addendum for updated specfications
2031	89	19.41	Technical Specs-Anti Phishing	Solution must provide granular administrative controls to allow role-based access to each module and quarantine folder.	Modern cloud-native anti-phishing solutions implement administrative segregation through configurable RBAC, delegated administration, role groups, and permission-based access models, which may not necessarily expose permissions at the individual module or quarantine-folder level Suggested Change Solution must provide granular administrative controls to allow role-based access	Please refer to the relevant Addendum for updated specfications
2032	89	19.43	Technical Specs-Anti Phishing	Solution must support complicated mail routing requirements, including group-based routing based on user groups	The requirement appears to address email infrastructure and mail-flow routing capabilities rather than core anti-phishing or email threat protection functionality. Complex mail routing, transport rules, and group-based routing are typically implemented within the email platform Suggested Change Remove this clause, its not applicable	Please refer to the relevant Addendum for updated specfications
2033	89	19.5 0	Technical Specs-Anti Phishing	solution must support a range of routing behaviors and actions for different scenarios, allowing administrators to customize email handling based on specific needs and requirements.	The requirement is broad and appears to focus on email routing and mail-flow management capabilities, which are typically functions of the email infrastructure (Microsoft Exchange, Exchange Online Suggested Change Remove this clause, its not applicable	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2034	90	19.51	Technical Specs-Anti Phishing	Solution must support for in outbound or inbound email including footer management Inserting one or more legal or compliance footers (e.g. disclaimer) Multi-language support Apply different filters based on email attributes or active directory attributes, Insert dynamic content to footer such as date, when to apply the footer in the message routing hops, Selectively apply based on policy / attribute or not apply if the email is s/mime encrypted or digitally signed, etc Apply signatures and disclaimers based on AD user groups	Footer management is vendor specific feature Suggested Change Remove the clause	Please refer to the relevant Addendum for updated specfications
2035	90	19.5 3	Technical Specs-Anti Phishing	Solution must allow end-users to receive customized email notifications based on domain name.	The clause prescribes a specific notification customization method (domain-based) that may not be supported by all modern cloud-native Anti-Phishing solution Suggested Change: Solution must allow end-users to receive customized email notifications based alerts, and awareness messages based on organizational policies	Please refer to the relevant Addendum for updated specfications
2036	90	19.5 7	Technical Specs-Anti Phishing	Solution must provide administrators with capabilities for email queue management	This feature is excahnge or onprim gateway specific. Suggested Change Remove the clause	Please refer to the relevant Addendum for updated specfications
2037	90	19.5 9	Technical Specs-Anti Phishing	Solution must support alerting the security team on all policies, quarantine folders, and queue thresholds	The clause is a gateway-specific alerting model based on quarantine folders and queue thresholds. Modern cloud-native email security solutions may not utilise traditional mail queues while still providing comprehensive alerting for security incidents, policy actions, quarantine events, and operational status Suggested Change Solution must support alerting the security team on all policies, quarantine folders, and queue thresholds or equivalent alerting mechanism	Please refer to the relevant Addendum for updated specfications
2038	90	19.6 2	Technical Specs-Anti Phishing	Solution must provide application and message routing troubleshooting tools with a message-tracing capability to facilitate help desk work	Message routing trobleshooting & message-tracing capabilities are part of exchange provider. Suggested Change Remove the clause	Please refer to the relevant Addendum for updated specfications
2039		Clause 23.1		The bidder shall perform review of Email solution twice in a year from Cert-IN empaneled organization and compliance verification shall be conducted within 2 months from the report submission.	Kindly clarify whether the bi-annual review is restricted to Web Application & Infrastructure VAPT of the email simulation portal, or if it mandates a comprehensive architecture configuration, mail security review, and source-code audit. Also, please confirm if the CERT-In empaneled auditor cost must be bundled into the simulation commercial bid.	Please refer addendum for revised clause.
2040		Clause 23.2		The platform should provide a separate dashboard for monitoring of DMARC/DNS Monitoring for Bank's Email solution.	Please clarify whether the bidder is expected to provide a full-fledged enterprise DMARC/DNS SaaS analytics module for the Bank's production corporate email domains, or if this refers solely to monitoring SPF/DKIM/DMARC delivery status for domains deployed during simulation exercises.	Please refer addendum for revised clause.
2041		Clause 18 & Clause 16	Bidder shall ensure that there is no restriction in number of phishing emails, number of calls, number of SMS to perform simulated phishing, vishing, smishing.		Please provide the estimated total employee head-count (user base) and an indicative annual campaign frequency/volume for automated calls (Vishing) and SMS (Smishing).	The Bidder shall size and quote the service based on the complete Bank user base. The Bank may conduct campaigns for the required users during the contract period. The Bidder shall ensure that the proposed service is scalable to meet the Bank's requirements.
2042		Clause 14	For conducting vishing using manual approach, each exercise shall be targeted for 100 employees per month.		Please confirm the expected call duration, script complexity, number of retries per unreached employee, and whether dedicated bilingual caller resources are required to be deployed on-site or can operate remotely.	Details shall be discussed with the successful bidder on case to case basis
2043		Clause 19.3 (a, h)		Developing look alike mobile application (Android and IOS) for phishing attack... Executables for Phishing attack need to be provided by the Bidder.	Please clarify whether mobile simulation involves actual distribution of dummy application binaries (APK/IPA via MDM/sideloading) or mock mobile-responsive web landing pages. If native binaries are mandated, please confirm Bank's MDM/enterprise whitelisting support.	The requirement is for conducting phishing simulations through mobile application-based attack scenarios. The Bidder shall provide the required executables/binaries for the proposed Android and iOS simulation, as applicable. The deployment/distribution mechanism shall be finalized in coordination with the Bank, considering the Bank's applicable security and device-management policies.
2044		Clause 23.7 & Clause 23.5		For Phishing activity, the bidder should not store any bank data in vendor location, data storage shall be restricted only on Bank network... updation of new features and upgradation of on-premise platform automatically from time-to-time.	Please clarify the approved deployment architecture: is the solution mandated to be purely On-Premise / Private Cloud within Bank DC/DR, or is an Indian MeitY-empaneled secure SaaS setup permitted? If on-premise, will the Bank provide the required VM, OS, and storage infrastructure?	Please refer addendum for revised clause.
2045		Clause 23.4		The bidder should provide 24*7 support (over call)... In case, the issue is not resolved for more than 8 hours, support personnel should visit Bank's CISO Office at Mumbai or at Hyderabad to resolve the issue.	Kindly confirm if the physical visit requirement applies strictly to Critical (P1) platform-down outages rather than minor campaign scheduling requests, and whether remote triage via secure VPN is permitted prior to physical engineer mobilization.	Please refer addendum for revised clause.
2046		RFP Functional Scope (AI Engine)		AI-based detection and classification of phishing and impersonation threats; AI-based correlation of exposed credentials, data leaks, and threat indicators.	Please clarify whether the AI module is required to perform inbound active email defense/inspection (analyzing external malicious emails targeting bank mailboxes) or if it is strictly meant for behavioral susceptibility scoring and simulation campaign adaptation.	Clause is not referring to this RFP
2047		Clause 21.6		Post completion of Cyber Awareness training module, user to undergo Cyber Awareness training Assessment to understand the effectiveness of the training program.	Please confirm if the assessment questions need to be auto-triggered immediately post-training within the platform, and whether scores must be exported/synced with the Bank's central HRMS/LMS via SCORM/xAPI connectors.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2048		Scope & S.No 1		Continuous discovery, identification, monitoring, classification, and risk assessment of the Bank's external and internal attack surfaces... All data collated from public domain via passive/non-intrusive scans.	Kindly clarify the scope of 'internal attack surface' discovery. Given that S.No 1 and S.No 41 mandate non-intrusive passive public-domain scans without software agents or dedicated on-premise hardware, please confirm if internal discovery is out of scope for the offsite ASM tool or if the Bank will provide read-only API feeds/connectors from internal scanners.	No Change, Please be guided by the RFP
2049		S.No 20 & S.No 22	The solution should automatically discover the bank's assets exposed to internet, including the assets of all the entities owned by and related to bank such as overseas branches, subsidiaries, third-parties, mergers, acquisitions etc.		Kindly provide the approximate initial inventory size (number of primary domains, CIDR netblocks/IP ranges, subsidiaries, and critical third parties) to be seeded for attack surface discovery and asset licensing calculation.	No Change, Please be guided by the RFP
2050		S.No 36 & S.No 37		The solution shall provide the capability to identify and classify shadow IT and unknown assets and facilitate their assessment through integration with the Bank's Vulnerability Management solution.	Kindly specify the make and version of the Bank's existing Vulnerability Management solution (e.g., Tenable.io/SC, Qualys, Rapid7) and whether direct API integration or normalized CSV/JSON push/pull is expected.	Details shall be shared with successful bidder
2051		Section 7.4.3 (p.55-56)		Offsite Managed Service: Continuous / 24×7 monitoring; Weekly discovery/update; Monthly reporting; Data localization in India.	Please confirm if the ASM solution can be deployed on an Indian MeitY-empaneled cloud (AWS/Azure/GCP India region) ensuring 100% data residency within India, or if an on-premise instance in the Bank's DC is strictly required.	No Change, Please be guided by the RFP
2052		S.No 7 & S.No 16	The bidder should offer unlimited number of take down services during the contract period... tie-ups with Browser providers such as Google, Mozilla, Microsoft and agencies like Cert-In for blocking the phishing sites.		Please provide the historical volume or expected annual baseline of takedown requests (phishing domains, rogue social media handles, rogue mobile apps) experienced by the Bank in previous years.	details shall be shared with successful bidder
2053		S.No 14		The Bidder should report the Bank within 1 hour of detection... The Bidder should be able to take down/shut down the phishing/brand abuse website/rogue application within agreed SLA upon Bank's confirmation, irrespective of geography.	While the bidder commits to initiating takedowns within agreed response SLAs, actual time-to-takedown depends on external global registrars, international ISPs, and hosting abuse teams. We request the Bank to define SLAs based on 'Takedown Initiation & Submission of Evidence' rather than absolute external hoster shutdown time.	No Change, Please be guided by the RFP
2054		S.No 16 (Compliance: C)		The bidder needs to have tie-ups with Browser providers such as Google, Mozilla, Microsoft and agencies like Cert-In for blocking the phishing sites.	Please clarify if integration via standard browser anti-phishing feeds (e.g., Google Safe Browsing API, Microsoft SmartScreen reporting, APWG feeds) and active reporting mechanisms to CERT-In satisfies the requirement of 'tie-ups'.	Please refer addendum for revised clause.
2055		S.No 22 (Compliance: Select)		The Bidder/OEM should be member of Anti-Phishing Working Group (APWG).	Kindly confirm if APWG OEM membership certificate or an equivalent international cybersecurity industry affiliation (e.g., FIRST, FS-ISAC, or authorized CERT-In coordination) is acceptable.	Please refer addendum for revised clause.
2056		S.No 33 (Compliance: C)		Search engines (like Google, yahoo, bing etc.) listing frauds where the customer care number & branch address of banks is changed/ modified should be continuously tracked and the same should be brought down immediately including Truecaller and JustDial.	Please clarify whether the Bank expects automated monitoring and remediation escalation via legal brand takedown notices, and whether the Bank will grant official Letter of Authorization (LOA) to the bidder to dispute fraudulent entries directly with Google Business Profiles, JustDial, and Truecaller.	Please refer addendum for revised clause.
2057		S.No 13 & S.No 24		Monitoring of rogue apps on AppStore like Google Play, Apple Store etc... fraudulent mobile applications targeting Client customers.	Please specify if the scope of mobile app monitoring extends beyond official app stores (Google Play, Apple App Store) to third-party APK repositories (e.g., APKPure, Aptoide), regional app marketplaces, and illicit Telegram channels distributing malicious banking trojan APKs.	No Change, Please be guided by the RFP
2058		S.No 6 & S.No 20		The platform should offer Top Executives/VIP account monitoring... Identification of account impersonation activity.	Kindly specify the maximum number of Key Executives / VIP personas (e.g., MD & CEO, EDs, Board Members, CISO) to be enrolled for VIP identity monitoring and social media impersonation tracking.	
2059		S.No 4 & S.No 28 (Compliance: C)		The solution shall provide advanced search capabilities through GUI and APIs using keywords, Threat Actors, Malware Families, Campaigns, CVEs, TTPs, C2 Infrastructure, IOCs, Countries and Industry sectors.	Please clarify if direct GUI search across raw dark-web/underground forum archives is required for Bank analysts, or if curated/threat-actor enriched feeds and analyst-validated search results fulfill the requirement.	Clarification: Curated, enriched and analyst-validated intelligence/search results shall be acceptable
2060		S.No 7 & S.No 10		The solution shall continuously monitor cyber threats associated with the Bank, subsidiaries, overseas branches, brands, third parties and digital assets... Banking, Financial Services, Insurance and Payment ecosystems.	Kindly share the indicative count of corporate email domains, BINs (Bank Identification Numbers), sub-entities, and critical third-party vendors to be continuously tracked for credential leaks and breach mentions.	Details shall be shared with successful bidder
2061		S.No 11, 26, 46 & Scope		Detect leaked credentials including usernames, passwords, session tokens, cookies, API Keys and Secrets... Data masking / tokenization of sensitive customer/bank data.	Please confirm if customer credential monitoring is expected in addition to employee corporate email credentials, and whether the Bank will provide hashed customer identifiers (or BIN prefixes) to facilitate targeted breach correlation while strictly complying with PII masking guidelines.	The requirement shall include monitoring of Bank/customer-related information.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2062		S.No 48 & S.No 49	Correlate intelligence with MITRE ATT&CK techniques... Support enrichment using CVE, CVSS v4.0, EPSS, CISA KEV and other industry-recognized threat intelligence sources.		Please clarify whether the threat intelligence platform is expected to export standardized feeds in STIX/TAXII format to integrate directly with the Bank's SIEM/SOAR/TIP (Threat Intelligence Platform), and specify the target SIEM/SOAR tool.	No Change, Please be guided by the RFP
2063		S.No 50 & S.No 53		Monitor and identify supply-chain threats affecting the Bank and critical third-party vendors... identify the source of the data breach, including third-party sources.	Kindly clarify if third-party supply-chain monitoring requires an automated Third-Party Cyber Risk Rating / Questionnaire assessment module, or if it is restricted to threat intelligence / leak monitoring mentioning designated vendors.	The requirement is intended to cover monitoring of supply-chain threats affecting the Bank and its critical third-party vendors, including relevant intelligence and information
2064		Offsite Managed Services (All Modules)		24x7 Continuous monitoring, Offsite Managed Service, monthly/weekly reporting, immediate critical alerts.	Kindly clarify if the Bank requires dedicated offsite L1/L2 security analysts exclusively assigned to the Bank, or if a shared 24x7 Managed Threat Intelligence & Monitoring Desk (SOC) providing dedicated SLA-driven deliverables is acceptable.	No Change, Please be guided by the RFP
2065		Data Localization & Compliance		Data localization in India; 2FA mandatory; Capable of integrating with Bank's existing Multi-Factor Authentication (MFA).	Please confirm that hosting the SaaS platforms in MeitY-empaneled Tier-III/IV Cloud Data Centers located physically within India fully satisfies the Bank's and RBI's data localization requirements, and confirm the Bank's IdP protocols for MFA (SAML 2.0 / OAuth / OIDC).	No Change, Please be guided by the RFP
2066	30, 34	7.2.1 Deployment Model & HA (TIP) / 7.2.4.1 Deployment Pattern	Table 7.2.1 Sr. 7; Cl. 7.2.4.1(e)	"Threat Intelligence Platform (TIP) - Cloud (SaaS) + Hybrid - Bank Location: Broker/Collector/Integrator: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR" (Table 7.2.1).	Cyble's Threat Intelligence Platform (TIP) is delivered as a fully cloud-native SaaS solution, providing continuous threat-intelligence aggregation, enrichment and distribution to the Bank via API, STIX/TAXII feed and a dedicated web portal, with high availability, geographic resiliency and disaster recovery built into the SaaS platform itself - fully aligned with the SLA, RTO and RPO defined in Section 13. As the TIP's core function requires no packet-level or in-line processing within the Bank's network, Cyble can meet the Bank's continuity requirement for this solution without deploying a broker/collector component on Bank premises. We request the Bank's confirmation that this cloud-native delivery model will be accepted as fully compliant with Table 7.2.1.	Please refer addendum for the revised deployment requirement
2067	31, 35	7.2.1 Deployment Model & HA (CSPM) / 7.2.4.1 Deployment Pattern	Table 7.2.1 Sr. 11; Cl. 7.2.4.1(i)	"Cloud Security Posture Management (CSPM) - Cloud (SaaS) + Hybrid - Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR" (Table 7.2.1); "...with the required connectors, collectors, agents, enforcers and/or other supporting Bank-side components, if required, deployed at the Bank's DC and DR in N+N Active-Active configuration" (Cl. 7.2.4.1(i)).	Cyble's Cloud Security Posture Management (CSPM) module continuously assesses the Bank's cloud environments through secure, read-only, API-based/cross-account IAM-role integration, with no agent, connector or collector required on Bank premises. This lets Cyble deliver continuous, real-time cloud security posture monitoring with high availability and resilience built natively into the SaaS platform, fully meeting the Bank's SLA, RTO and RPO requirements under Section 13. This is consistent with the qualifying language "if required" already present in Cl. 7.2.4.1(i). We request the Bank's confirmation that this API-integrated, cloud-native delivery model will be accepted as compliant.	Please refer addendum for the revised clause
2068	55-56	7.4.3 Attack Surface Management	Cl. 7.4.3	"Discovery of internet-facing and internal assets... The proposed solution shall provide AI-enabled Attack Surface Management (ASM) capabilities for continuous discovery... of the organization's external attack surface, including known and unknown internet-facing assets."	Cyble's Attack Surface Management (ASM) capability provides continuous, AI-enabled discovery, monitoring and risk-prioritization of the Bank's entire external attack surface - internet-facing assets, exposed services, domains, cloud assets and shadow IT - using external/passive reconnaissance together with Bank-shared asset inventories (IP ranges, domains, cloud accounts), with no agent or appliance required inside the Bank's network, consistent with the offsite Managed Service model in Section 7.2.2. This gives the Bank a complete outside-in exposure view from Day 1. We request the Bank's confirmation that this externally-led, agentless approach satisfies Cl. 7.4.3.	Bank is looking for external attack surface management
2069	55	7.4.5 Anti-Phishing	Cl. 7.4.5	"...offsite continuous anti-phishing monitoring and response services for detection, analysis for phishing attacks targeting the Bank, its employees, customers, executives, digital assets, domains, and online channels."	Cyble is fully equipped to deliver continuous, 24x7 Anti-Phishing monitoring across the Bank's domains, executives and digital channels from Day 1 of the engagement, scaling seamlessly as the Bank's digital footprint grows, with no additional infrastructure required from the Bank. To finalise the onboarding plan, we request the Bank share the number of primary/registered domains, sub-domains, executive/VIP identities and customer-facing digital channels to be covered at contract commencement, so Cyble can confirm precise sizing against this scope.	Please refer to the relevant Addendum for updated specfications
2070	57	7.4.6 Dark Web Monitoring	Cl. 7.4.6	"...offsite, tool-based continuous dark web and cyber threat exposure monitoring services... across the surface web, deep web, dark web, underground forums, messaging platforms, and data leak repositories."	Cyble's Dark Web & Cybercrime Monitoring capability continuously covers the surface web, deep web, dark web, underground forums, messaging platforms and data-leak repositories, and can begin protecting the Bank's specified identities, brand keywords and domains immediately upon contract signature. To tailor this coverage precisely, we request the Bank share the initial monitoring scope (employee/executive identities, brand keywords, domains and relevant data categories) so Cyble can confirm sizing and reporting cadence.	Details shall be shared with succesful bidder
2071	57	7.4.7 Threat Intelligence Feed	Cl. 7.4.7(l)	"Provision of threat intelligence through a centralized portal/dashboard and/or machine-readable feeds."	Cyble's Threat Intelligence Feed is delivered through both a centralized portal/dashboard and machine-readable, standards-based feeds (STIX/TAXII, MISP-compatible formats and API), enabling seamless integration with the Bank's existing or future security stack whenever required. We confirm this dual delivery model - portal-based consumption plus machine-readable feed/API - and request the Bank's confirmation that it satisfies Cl. 7.4.7.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2072	57-58	7.4.8 Threat Hunting Services	Cl. 7.4.8(m)	"The threat hunting service shall be delivered remotely/offsite using secure and mutually agreed mechanisms for accessing relevant logs, telemetry, security tools, and data made available by the Bank."	Cyble can deliver proactive, intelligence-driven Threat Hunting entirely offsite - correlating curated external threat intelligence (IOCs, IOAs, TTPs, threat-actor and campaign intelligence) against Bank-shared context, supplemented by secure, mutually agreed read-only access to relevant Bank telemetry for validation and deeper investigation as needed - fully consistent with the remote/offsite delivery model mandated in Cl. 7.4.8(m). We request the Bank's confirmation that this intelligence-led hunting model, combined with agreed read-only telemetry access, meets the Bank's requirement.	No Change, Please be guided by the RFP
2073	58	7.4.9 Brand Protection and Monitoring	Cl. 7.4.9(j)	"Takedown coordination with relevant registrars, hosting providers, platforms, application stores, social media platforms, and other relevant entities, wherever applicable."	Cyble's Brand Reputation Monitoring capability continuously identifies brand impersonation, typosquatting, phishing/fraudulent websites, fraudulent mobile apps and social-media impersonation, and actively coordinates takedown requests with registrars, hosting providers, app stores and social platforms on the Bank's behalf under a standard authorisation executed at contract signature - delivering a fully managed, end-to-end takedown process with minimal effort required from the Bank's team. We request the Bank's confirmation that this bidder-led takedown coordination model satisfies Cl. 7.4.9(j).	Please refer addendum for revised clause
2074	256	16.21 Annexure 21: Sizing/Volumetrics (gap for Offsite Services)	Annexure 21, Sizing table	Annexure 21's sizing table provides explicit volumetrics (EPS, endpoint counts, IPs, VPCs, etc.) for the 14 solutions under Section 7.3, but no equivalent executive/VIP count is specified for the offsite services that monitor executive exposure (Anti-Phishing - Cl. 7.4.5, Dark Web Monitoring - Cl. 7.4.6, Brand Protection - Cl. 7.4.9).	Cyble's Executive Monitoring and Digital Risk Protection capabilities can protect any number of the Bank's executives/VIPs from Day 1, with coverage scaled precisely to the Bank's requirement across Anti-Phishing, Dark Web Monitoring and Brand Protection. To finalise sizing, we request the Bank confirm the number of executives/VIPs (e.g., Board members, CXOs, senior management) to be brought under continuous monitoring at contract commencement.	Please refer to the relevant Addendum for updated specfications
2075	256	16.21 Annexure 21: Sizing/Volumetrics (gap for Offsite Services)	Annexure 21, Sizing table	As above - no domain/sub-domain count is specified for the offsite services that monitor the Bank's external digital footprint (Attack Surface Management - Cl. 7.4.3, Anti-Phishing - Cl. 7.4.5, Brand Protection - Cl. 7.4.9).	Cyble can bring any number of the Bank's domains and sub-domains under continuous monitoring across Attack Surface Management, Anti-Phishing and Brand Protection from Day 1. To finalise sizing, we request the Bank confirm the number of primary domains and sub-domains to be monitored at contract commencement, and the expected annual growth in this count.	details shall be shared with successful bidder
2076	54	7.4 Functional Requirement - Services (Offsite Services)	Cl. 7.4(d)	"The Bidder shall implement appropriate security controls, including data masking or tokenization for sensitive data, Role-Based Access Control (RBAC), Just-in-Time (JIT) privileged access, and comprehensive audit logging for all services delivered under this RFP." - no named-user/license count is specified for platform/dashboard access to the 9 offsite services.	Cyble's platform can be provisioned for any number of the Bank's analysts, CISO-office and compliance stakeholders who need dashboard access to the offsite services, with full role-based access control as required under Cl. 7.4(d). To size the commercial bid precisely, we request the Bank confirm the number of named analyst/console user licenses required for the Bank's teams to access Cyble's platform and reporting for the proposed offsite services.	details shall be shared with successful bidder
2077	55, 58	7.4.5 Anti-Phishing / 7.4.9 Brand Protection and Monitoring	Cl. 7.4.5; Cl. 7.4.9(j)	Neither clause, nor Annexure 21, specifies an expected volume of takedown actions per month/year for phishing sites, fraudulent domains, or fake social media/mobile app listings.	Cyble is fully equipped to execute takedown actions at whatever volume the Bank's threat exposure requires. To align commercial terms precisely with the Bank's risk profile, we request the Bank confirm the estimated number of takedown actions (phishing sites, fraudulent domains, fake social media/mobile app listings) expected per month under Anti-Phishing and Brand Protection.	Please refer to the relevant Addendum for updated specfications
2078	Page 7	1	Bid validity	180 days from the date of opening of the bid.	We request you to change this to 15 days or as per validity given by OEMs	No Change, Please be guided by the RFP
2079	Page 16	6.2	Bid Currency & Price Structure	Prices shall be expressed in the Indian Rupees only. The bidder must quote price exclusive of all applicable GST. The cost will not depend on any variation in the dollar exchange rate/change in tax structure.	Bidder will quote based on the current cost price of the quoted products and current exchange rate. Due to the current global uncertainty concerning the proposed US tariffs, and the fluctuating foreign exchange rates, our quoted price will subject to change based on the then current exchange rate and any associated vendor price increases at the time of invoicing. Pls confirm	No Change, Please be guided by the RFP. Refer section 6.2, 6.3, and clause 6.20
2080	Page 97	8	Contract Period	The bank may, at its sole discretion, extend the contract for an additional period of two years, in one year increments tranches. The Bank may extend the support services for an additional period of up to two (2) years beyond the original contract period. The pricing applicable during the extension period shall be mutually agreed and shall not exceed 120% of last year's AMC/ATS/Facility management rates quoted by the Selected Bidder.	Over a five-year period, market conditions may change significantly. Extending the contract on the same commercial and legal terms may not reflect the prevailing market realities at the time of extension, potentially leading to financial unviability for the service provider hence we request PSB to mutually discuss and agree upon the terms and commercials at the time of extension or renewal.	No Change, Please be guided by the RFP
2081	Page 158	13.3	At-Risk Amount	The monthly At-Risk Amount (ARA') shall be 15% of the estimated monthly payout of the respective month.	We request the Bank to kindly waive the At-Risk Amount (ARA) provision, as bidder performance is already governed through the SLA/KPI framework and associated service credits/penalties. Accordingly, monthly invoices may be released as per agreed payment terms, subject to applicable SLA adjustments, without additional retention of ARA.	The At-Risk Amount is a contractual performance mechanism and shall be withheld/adjusted in accordance with the applicable performance requirements specified in the RFP. It shall not automatically be treated as an additional penalty or Liquidated Damages (LD). Any withholding, adjustment or recovery under the At-Risk Amount shall be accounted for within the overall 10% penalty/LD cap specified in Section 13.2 and shall not be over and above such cap.
2082	Page 159	14.2	Right to Alter quantities	The bank reserves the right, at the time of award of contract and/or during the currency of the contract, to increase or decrease the quantity of goods, licenses, subscriptions, appliances, equipment, services, implementation effort, support services, or any line item covered under the contract by up to twenty five percent (25%) of the quantities specified in the RFP/Contract, without any change in the unit prices, terms and conditions, technical specifications, delivery schedule, warranty obligations, support commitments, or any other contractual conditions.	We request that any increase in scope, quantities, quantity of goods, licenses, subscriptions, appliances, equipment, services, implementation effort, support services, or any line item covered under the contract in the RFP be treated as a change request and be priced separately. Any increase shall be undertaken at mutually agreed rates prevailing at the time of such increase.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2083	Page 159	14.2	Right to Alter quantities	The bank reserves the right, at the time of award of contract and/or during the currency of the contract, to increase or decrease the quantity of goods, licenses, subscriptions, appliances, equipment, services, implementation effort, support services, or any line item covered under the contract by up to twenty five percent (25%) of the quantities specified in the RFP/Contract, without any change in the unit prices, terms and conditions, technical specifications, delivery schedule, warranty obligations, support commitments, or any other contractual conditions.	Our commercial quote is based on a minimum committed quantity. A reduction in order size impacts pricing viability. Hence, we request that the minimum committed quantity not be reduced, or that any reduction be done only with mutual consent.	No Change, Please be guided by the RFP
2084	Page 165	14.19	Liquidated Damages	If the bidder fails to deliver any or all of the products and/or systems and/or services solutions within the time period(s) specified in the Delivery Schedule or installation, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 0.5 percent per week or part thereof of Contract Price subject to maximum deduction of 10% of the total contract value, until actual delivery, installation or performance as per related clauses mentioned in RFP.	Request Bank to amend the LD clause as follows: "Liquidated Damages shall be levied at 0.5% per week of value of the delayed portion of the deliverables, subject to a maximum of 5% of the value of the affected milestone. Delays attributable to the Bank, its agents, third parties, OEM dependencies, force majeure events, site readiness issues, delayed approvals/sign-offs, or reasons beyond the bidder's reasonable control shall be excluded for computation of LD."	No Change, Please be guided by the RFP
2085	Page 166	14.22	Order Cancellation	The Bank reserves its right to cancel the entire unexecuted part of the Purchase Order at any time on its convenience without assigning any reason/s whatsoever.	We request Bank if the contract is terminated for convenience,PSB shall additionally pay to the Bidder for all work done till the date of termination, as well as for the orders already placed with OEMs/Licensors, which orders cannot be cancelled with the OEMs/Licensors, cancellation costs, if any, levied by the OEMs/Licensors, and logistical and administrative expenses, if any, incurred by the Bidder on account of such cancellations, which expenses shall be billed on actuals. Further, if the Bidder is providing any products/goods on opex or lease model, then PSB shall pay the Bidder the residual value of the products.	No Change, Please be guided by the RFP
2086	115	12	Payment Terms	Payment Terms	WE request bank to change the payment terms as follows:-	No Change, Please be guided by the RFP
2087	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 23	SIEM	Point 18	The proposed solution shall provide cloud-native high availability and redundancy mechanisms to tolerate failures of underlying infrastructure components without disruption to security monitoring and operational capabilities. The solution shall provide automated failover and service continuity within the cloud environment through the CSP's native availability and resiliency capabilities	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. "" The proposed solution shall provide cloud-native redundancy mechanisms to tolerate failures of underlying infrastructure components without disruption to security monitoring and operational capabilities. The solution shall provide automated failover and service continuity "	Please refer the addendum for revised clause
2088	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 23	SIEM	Point 36	The proposed solution must come with out-of the-box/customized to be delivered on day 1 support integration and dashboards, reports, rules etc. to provides rapid insights and operational visibility into large-scale CentOS, Windows, Unix and Linux environments machine data.: syslog, metrics and configuration files.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The proposed solution must come with out-of the-box/customized to be delivered on day 1 support integration and dashboards, reports, rules etc. to provides rapid insights and operational visibility into large-scale CentOS, Windows, Linux environments machine data.: syslog, metrics and configuration files.	No Change, Please be guided by the RFP
2089	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 24	SIEM	Point 59	The proposed solution machine learning capabilities must allow addition or have inbuilt feature of custom machine learning algorithms from popular open-source libraries like NLP, Python etc.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The proposed solution must natively supports custom machine learning algorithms through its built-in Bring Your Own Machine Learning (BYOML) framework. This capability allows mature Security Operations Centers (SOCs) and security data scientists to access the massive security data lake stored within the platform and run bespoke analytics tailored to their specific environment.	No Change, Please be guided by the RFP
2090	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 37	XDR	Point 43	The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature or through seamless integration with a third-party sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature or through seamless integration with a third-party sandboxing solution from day 1.""	Please refer the addendum for revised clause
2091	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 1.4	Identity Threat Detection Solution must find and present high-risk attack pathways to critical IT assets	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. "ITDR provides identity risk context through User Risk View, Risk Management Dashboard, and identity alerts.	Please refer the addendum for revised clause
2092	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 1.6	Identity Threat Detection Solution should must automatically prioritize and remediate the riskiest identities to preemptively cut off what attackers need (and expect to find) to move undetected within the network.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. "ITDR identifies risky identities and supports remediation workflows for suspicious identity activity."	Please refer the addendum for revised clause
2093	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.3	The ITDR solution shall identify and assess exposed, improperly stored, or compromised credentials associated with user, privileged, service, and administrative identities on endpoints	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ITDR identifies risky identity posture, weak or compromised credentials, and suspicious activity involving user, privileged, service, and administrative accounts.	Please refer the addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2094	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.4	Identity Threat Detection Solution should Identify, Misconfigured accounts, Legacy app accounts, Stale accounts, password policy violations, Kerberoastable credentials, unmanaged user accounts, unmanaged service accounts	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR identifies risky identity posture, weak or compromised credentials, Kerberoasting activity, and suspicious behavior involving service and administrative accounts""	Please refer the addendum for revised clause
2095	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.5	Identity Threat Detection Solution should Provide continuous monitoring and customizable, automated business rules to eliminate security policy violations, such as: • Stored credentials to sensitive assets • Local-admin accounts • Cached credentials stored in browsers, Windows and other systems	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR continuously monitors identity posture and access relationships to identify risky configurations, excessive privileges, and suspicious identity activity across Active Directory and related identity sources.""	Please refer the addendum for revised clause
2096	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.7	Identity Threat Detection Solution should be available through rack-mountable on-premise deployment	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Identity Threat Detection Solution should be available through rack-mountable on-premise deployment not applicable for SaaS solution ""	Please refer the addendum for revised clause
2097	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.9	Identity Threat Detection Solution should detect all types of attack vectors including but not limited to pre attack reconnaissance,zero- day attacks, privilege escalation prevention, lateral movement, data theft	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR detects identity-based threats such as Active Directory reconnaissance, compromised accounts, privilege escalation, and anomalous access, while providing identity context to help investigate exposure and attack paths.""	The Clause is applicable only to idendity related threat vector only. The volumetrics is provided in the RFP and should be complied
2098	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.15	Identity Threat Detection controls should be able to automatically discover and flag hidden or shadow Tier 0 assets	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Identity Threat Detection and Response helps identify risky identity assets, excessive privileges, and exposure across identity relationships.""	Please refer the addendum for revised clause
2099	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.17	Identity Threat Detection Solution should be able to pull and analyze identity data from AD, Entra ID, identity stores, PAM systems	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR analyzes identity data from supported identity sources, including Active Directory and Microsoft Entra ID, to provide context on identities, permissions, and access exposure""	Please refer the addendum for revised clause
2100	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 3.4	The Identity Threat Detection Solution should integrate with compatible endpoint/extended detection solution to capture screen recordings or screenshots during active attacker sessions, as part of advanced forensic evidence collection	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR integrates with supported tools to share identity and endpoint context for investigation and response, including forensic collection where available.""	Please refer the addendum for revised clause
2101	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 3.5	The Identity Threat Detection Solution should integrate with compatible network detection solution to support collection of PCAP data to support network-level visibility of the incident	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR integrates with supported tools to share identity risk context and support investigation workflows, including network-related telemetry where available.""	Please refer the addendum for revised clause
2102	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 53	ITDR	Point 3.7	Identity Threat Detection Solution should, as part of its forensic data collection process, include detailed attack path information, including the protocols leveraged during the attack.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR provides identity context through asset, permission, and authentication analysis, and detects identity-based threats such as compromised accounts, privilege escalation, anomalous access, and Active Directory reconnaissance.""	Please refer the addendum for revised clause
2103	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 53	ITDR	Point 3.9	Identity Threat Detection solution should detect an adversary's attempt to move laterally toward the organization's key assets using as many hosts (Windows, Mac, or Linux) as possible in the organization without requiring a persistent agent.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Identity Threat Detection solution should detect an adversary's attempt to move laterally toward the organization's key assets using as many hosts (Windows, Mac, or Linux) as possible in the organization With or without requiring a persistent agent.""	Please refer the addendum for revised clause
2104	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 53	ITDR	Point 3.10	Identity Threat Detection Solution should collect user and computer information from Active Directory as part of its forensic data gathering to enhance context and assess risk exposure. detect at the earliest point in the attack, post initial compromise as the attacker is first attempting to move laterally and escalate privilege.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR collects and analyzes identity data to improve context and assess risk exposure. It detects identity-based threats, including compromised accounts, privilege escalation, anomalous access, and Active Directory reconnaissance, early in the attack path.""	Please refer the addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2105	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 53	ITDR	Point 3.11	Identity Threat Detection Solution should collect user and computer data from Active Directory during forensic data gathering to improve context and evaluate risk exposure, while ensuring that all deception techniques remain hidden from legitimate users.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Identity Threat Detection and Response collects and analyzes identity data to improve context and assess risk exposure. It provides deep visibility into identity assets, permissions, relationships, and authentication activity across Active Directory and other identity sources. ITDR also supports forensic investigations through endpoint data collection and analysis."	Please refer the addendum for revised clause
2106	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 19	CTEM	Point 7	Each intelligence item should include metadata such as date, author, source, and pre-classification of raw data	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Intelligence items include enriched context, source information, and analysis metadata to support investigation and prioritization.'"	Please refer the addendum for revised clause
2107	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 19	CTEM	Point 11	The solution/service should generate investigation reports for designated VIPs or other high-risk identities/assets, providing an overview of identified digital exposure and associated risk.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution provides risk context and investigation views for identities and assets, helping analysts assess exposure and related risks.""	No Change, Please be guided by the RFP
2108	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 19	CTEM	Point 19	The solution should detect compromised credentials for employees and VIPs, exposed payment card information, and aggregate data from known breach databases in real time	Kindly Remove this clause for larger participation	Please refer addendum for revised clause
2109	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 20	CTEM	Point 38	The solution should be deployed agentlessly, without requiring sensors or agents on endpoints, servers, or network appliances	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution should be deployed agentlessly, With or without requiring sensors or agents on endpoints, servers, or network appliances""	S.No 38 Please refer addendum for revised clause The solution should be deployed agent/agentlessly, without requiring sensors or agents on endpoints, servers or network appliances.
2110	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 81	ASM	Point 6	The visual representations should be downloadable in PDF, JPG, PNG and other generally used formats	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution supports exporting reports and data views in supported file formats such as PDF, CSV, TSV, JSON, or ZIP, depending on the workflow""	No Change, Please be guided by the RFP
2111	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 81	ASM	Point 8	The solution shall provide information on vulnerabilities, misconfigurations, insecure configurations, obsolete or unsupported technologies, applications, services, URLs, ports, network components, systems, databases and other relevant infrastructure that are publicly exposed or otherwise identifiable through authorized discovery and assessment activities.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution provides exposure information for internet-facing assets, including vulnerabilities, misconfigurations, services, and related attribution data discovered through authorized asset mapping and assessment.""	Please refer addendum for revised clause
2112	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 81	ASM	Point 9	The solution should provide data/information on security flaws/ inherent vulnerabilities (allegedly) reported about the digital products exposed to the Internet (For example: internet banking, mobile applications) offered to the bank's customers, as leaked in public domain, or other forums	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution provides exposure and risk information for internet-facing digital assets, including vulnerabilities, services.""	No Change, Please be guided by the RFP The requirement is intended to provide visibility not only into directly identified technical vulnerabilities but also into relevant security information concerning the Bank's internet-facing digital products
2113	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 81	ASM	Point 10	The solution shall identify and provide relevant information on potentially exposed sensitive information associated with the Bank, including source-code references, code snippets, API information, credentials, keys and other security-relevant information, where such information is identifiable through publicly available sources, external attack-surface intelligence or other authorized discovery mechanisms.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution provides exposure information for internet-facing assets, including vulnerabilities, misconfigurations, code weaknesses, and exposed secrets discovered through attack surface.""	Please refer addendum for revised clause
2114	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 54	Cloud security	Point 4	The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud environment like AWS/Azure/GCP/Meghdoot, AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud environment like AWS/Azure/GCP/, AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.	The requirement is intended for identification and contextualization of potentially exposed sensitive information associated with the Bank
2115	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 55	Cloud security	Point 9 (Sub point)	○Automatic, in-product remediation via the Cloud Service Provider (CSP) API (1-click)	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution supports in-product remediation workflows, including automated actions and approval-based playbooks where configured.	Please refer the addendum for revised clause
2116	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 56	Cloud security	Point 25	The solution must provide an self-service portal for engineers. The admin portal should be able to define the eligibility for users and groups, based on role, scope and duration. The solution should provide approval workflow and audit logs	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation." The solution supports granular access control, human approval in select workflows, and audit logging for access-related changes.	Please refer the addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2117	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 40	NDR	Point 9	Easy-to-manage, clientless platform that deploys quickly and involves minimal or no dependency on customization and management.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Easy-to-manage, clientbase clientless platform that deploys quickly and involves minimal or no dependency on customization and management.""	Please refer the addendum for revised clause
2118	RFP Pg 35	Deployment Pattern	Point 9	NDR: The NDR solution shall be deployed On-Premises within the Bank's DC and DR, with the required brokers, aggregators, collectors and/or enforcement components configured in N+N Active-Active configuration at both sites.	The proposed NDR solution shall utilize a hybrid deployment model or SaaS model.With the required brokers/ aggregators/collectors /Sensors and enforcement components configured in N+N Active-Active or Active- Passive configuration at both sites DC and DR.	Please refer addendum for the revised clause
2119	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 40	NDR			Clarification: Kindly confirm the specific physical interface type and speed the Bank will provide for the uplink to the NDR sensor.	Details shall be shared with successful bidder
2120	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 40	NDR	Point 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	"We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. "" The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead.""	Please refer Addendum for revised clause
2121	SELECTION OF BIDDER FOR SUPPLY INSTALLATION, IMPLEMENTATION, MAINTENANCE & MANAGEMENT OF NEXTGEN SOC & RELATED SERVICES BID NO: PSB/ HO-CISO CELL/2026-27/RFP_01 DATED 09/09/2026 Page 68	7.7 On-cloud proposed solution OEM Responsibilities	Page 8	The solution shall support secure connectivity with the Bank's on-premises infrastructure,cloud environments, and external systems through private and secure communication mechanisms.	SIEM is a SaaS solution accessible over the internet using passwords and multi-factor authentication and Https. However, access to your Cortex XSIAM tenant can be restricted based on your Bank's static public IP addresses. Kinkdy change this clause to "" The solution shall support secure connectivity with the Bank's on-premises infrastructure,cloud environments, and external systems through private or secure communication mechanisms via internet or tenant can be restricted based on Bank's static public IP addresses.."""	Please refer the addendum for revised clause
2122	RFP Pg 33	Section 7.2.3 Deployment Model Definition		CSP-hosted components shall provide cloud-native High Availability (HA), geographic resiliency and DR in accordance with the SLA, RTO and RPO requirements specified in this RFP.	Cortex XSIAM is pure SaaS Solution hence this clause is not applicable. kindly remove this for SaaS offerings.	Please refer addendum for the revised deployment architecture
2123	RFP Pg 41	7.3.1.1 Modules, Architecture & Deployment:	Point 7	All SIEM components, including collectors, ingestion nodes, correlation engines, processing nodes, etc., are deployed in the prescribed HA architecture irrespective of whether they are deployed at the Bank's Data Centre (DC), Disaster Recovery (DR) Centre, CSP Primary Site, or CSP Secondary Site.	Not applicable, as Cortex XSIAM is a SaaS solution. However, the on-premises Cortex Broker VM component can be deployed in a High Availability (HA) configuration across primary Data Center (DC) and Disaster Recovery (DR) sites	For SaaS-based components, the applicable SaaS SLA shall specify the required uptime/availability commitment. For components deployed at the Bank's DC/DR, the prescribed HA architecture shall apply as specified in the RFP
2124	RFP Pg 43	7.3.2.2 Key Deliverables	Point 7	Backup, retention, restoration, documentation and knowledge transfer for configured security automation capabilities and use cases.	Need more clarification on this clause	No Change, Please be guided by the RFP Refer Section7.2.4.3 Storage and other Requirement
2125	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 2-11	Cloud CSP	3	The proposed cloud infrastructure should be deployed in High Availability mode (N+N) at both primary site and secondary site.	This clause is applicable only if the solution delivered via PaaS, Cortex XSIAM is pure SaaS Solution hence this clause is not applicable. Request you to change the clause "" The cloud infrastructure should have presence in at least 2 cities in India in different SEISMIC Zone OR Deliver 99.99 % uptime from a single cloud region ""	Please refer addendum for the revised clause
2126	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 2-11	Cloud CSP	4	The solution shall meet Bank-defined RPO/RTO and resilience requirements irrespective of the replication technology adopted.	This clause is applicable only if the solution delivered via PaaS, Since Cortex XSIAM is pure SaaS Solution Bank defined RTO RTO will not be applicable.	Please refer addendum for the revised clause
2127	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 2-11	Cloud CSP	10	OEM shall esnure compliance of the complete proposed solution & platform with RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and all applicable regulations throughout the contract period.	Kindly chage is to "" OEM shall esnure compliance of the complete proposed solution & platform with RBI, CERT-In, CSCRF,, IT Act, MeitY and all applicable regulations throughout the contract period.""	Please refer addendum for revised clause
2128	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 2-11	Cloud CSP	16	Solution provider should have capability to provide Alerts & Monitoring interface. Solution should support Remote Administration for administrators	This clause is applicable only if the solution delivered via PaaS, Cortex XSIAM is pure SaaS Solution hence this clause is not applicable. kindly remove this for SaaS offerings.	Please refer addendum for the revised clause
2129	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 2-11	Cloud CSP	18	The cloud infrastructure should have presence in at least 2 cities in India in different SEISMIC Zone	This clause is applicable only if the solution delivered via PaaS, Cortex XSIAM is pure SaaS Solution hence this clause is not applicable. Request you to change ths clause "" The cloud infrastructure should have presence in at least 2 cities in India in different SEISMIC Zone OR Deliver 99.99 % uptime from a single cloud region ""	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2130	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 2-11	Cloud CSP	163	The solution should be deployed on dedicated cloud instance for Bank. The Bidder shall finalize the cloud solution requirement in line with volume, request/response times, cloud replication requirements, back up disk & media based.	Kinldy chnage this clause to ""The solution should be deployed on dedicated cloud instance for Bank. The Bidder shall finalize the cloud solution requirement in line with volume, request/response times, cloud replication requirements""	Please refer addendum for revised clause
2131	29, 35 & 259	Sections 7.2.1, 7.2.4.1(b) & 16.21.2	Section 7.2.1 (	Deception deployment and high-availability topology Deception Technology): "Any agent/Enforcer/Deceptor Standalone at DC and HA, N+N, Standalone at DR." Section 7.2.4.1(b): "The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active configuration." Section 16.21.2 (Decoy): "All the inline components of the solution must operate in high availability mode. In the event of any component failure, the system should automatically initiate failovers within seconds, ensuring uninterrupted functionality without requiring manual intervention."	The RFP describes the Bank-side deception components as standalone in Section 7.2.1, point no.- 4, but it is also mentioned HA and N+N. We request the bank to kindly clarify that in case we're deploying the solution on-prem, whether Bank needs the solution in Standalone mode/HA mode/N+N mode. Section 16.21.2 (Decoy), point no.-8, Bank has asked that all the inline components of solution should be in HA mode with automatic failover capability. However, the deception solution is not inline. Hence, we request Bank to clarify if they need the Deception Solution in HA. We request the Bank to add on-prem solution also in addition to Cloud/SAAS+Hybrid.	Please refer addendum for revised clause
2132	45, 261 & 262	Sections 7.3.6.2(2) & 16.21.3 - Deployment and Data Retention	Section 7.3.6.2(2):	Backup, restoration and log-retention requirements "Restore the logs/data from backup for forensic investigation and as per bank requirement without any additional cost." Section 16.21.3: "Duration of the Contract (Monthly Full backup) - Long-Term Storage (LTS) - Entire Duration of the Contract." The RFP further states that applicable Monthly Full Backups shall be migrated to LTS at the Bank's DC & DR and retained for the entire duration of the contract.	We request bank to kindly confirm that if the bank will provide the storage for backup.	No Change, Please be guided by the RFP. Bidder to right size and provide all the required infrastrcuture as per RFP
2133	68	Section 7.7 - On-cloud proposed solution OEM Responsibilities, Point 10	"The OEM shall have valid ISO/IEC 27001 certification and SOC 2 Type II report."	Cloud OEM certification requirement	We request the bank to accept ISO/IEC 27001 or SOC 2 Type II or both.	No Change, Please be guided by the RFP
2134	29, 32 & 35	Sections 7.2.1, 7.2.3 and 7.2.4.1(b)	Section 7.2.1	Responsibility for providing the Cloud/SaaS environment (Deception Technology): "Cloud (SaaS) + Hybrid" Section 7.2.3: "The solution shall be hosted through a Cloud Service Provider (CSP), either fully as a SaaS service or through a combination of CSP-hosted and Bank-hosted components." Section 7.2.4.1(b): "Deception Technology: The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active configuration. The Cloud/SaaS deployment shall be aligned with the applicable SLA, RTO and RPO requirements."	7.2.4.1(b) We request the bank to kindly add the on-prem implementation option also for the core component of the Deception Solution.	Please refer addendum for revised clause
2135	35 & 91	Sections 7.2.4.1(b) and 7.18.1 - Compute Infrastructure, Point 1	Section 7.2.4.1(b):	Hardware and VM infrastructure for Bank-hosted deception components "Deception Technology: The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active configuration. The Cloud/SaaS deployment shall be aligned with the applicable SLA, RTO and RPO requirements." Section 7.18.1(1): "Bidders must design, size, supply, implement, maintain and manage suitable compute infrastructure for all the in-scope applications/solutions proposed in the RFP response."	We request the bank to kindly add the on-prem implementation option also for the core component of the Deception Solution.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2136	30	7.2.1 Solutions – Master Deployment Matrix	#8. Vulnerability assessment (VA) & vulnerability lifecycle management	Bank Location: Standalone at DC and Standalone at DR. Management Console: Deployed at both DC and DR	As per this RFP Technical Specification of VA & VLM,document #1788963129, #12 "The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and failover capabilities" where the 7.2.1 of suggests standalone deployment at DC, DR and console availablity at both DC and DR. These two partially contradict each other. We request you to kindly confirm if standalone VA & VM in DC and DR are expected to function independently. Maintaining two standalone environments with both consoles accessibility will lead to duplication of vulnerabilities, configuration efforts and it will cost upto 2X in terms of licensing. Though its not clear but we assume that you need one VM in DC and one in DR where primary one shares configuration backup on secondary and secondary can take over when the primary goes down, the primary VM solution should be able to scan both the DCs and vice-versa. If this understanding is correct, kindly update the clause as following - 'The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and active-cold standby failover capabilities where only one active console shall be accessible at a time'.	No Change, Please be guided by the RFP
2137	260	16.21.2 Volumetrics-Solution-wise Requirements	10 Vulnerability Assessment & Management (VA-VM) Minimum Numbers of IPs: 4000	10 Vulnerability Assessment & Management (VA-VM) Minimum Numbers of IPs: 4000	As per the RFP #1788963158, page 257 16.21.1 Current IT assets, P&SB has 2500 servers, 300 DB, 200 Apps, 12000 endpoints/desktops and 7200 routers and switches whereas the VA/VM IP coverage is mention as "Minimum" 4000. We seek your guidance and confirmation on the final count of assets/IPs you need coverage from day #1, given "minimum" count may lead to each bidder proposing seperate numbers and very likely excluding important assets from highly important VA & VM exercise. Without a defined and finite asset count, bidders cannot be compared on a like-for-like basis as the ones concerned about the VA/VM security posture of the infra will propose to cover more IPs/Assets while some may cover bare minimum and appear more competitive. We request you to kindly provide the final IP count required for VA/VM from day #1 considering the licenses are bound to assets and deleting the asset will delete all historic vulnerability and trends data, deleted asset will not cover alerts, ITSM integration and cannot be considered as part of VM exercise. As per the CERT'in recommendations (https://www.cert-in.org.in/PDF/guidelinesgovtentities.pdf) as well as industry best practices, entire ICT infrastructure should be part of the vulnerability management exercise and network device inclusion is absolute must given these are critical assets and in some zones exposed directly to internet.	No Change, Please be guided by the RFP
2138	38	On premises deployment of solutions	Storage Capacity & Sizing	• The Bidder shall provide detailed storage sizing based on expected data/log volumes, peak ingestion rate, retention period, indexing, enrichment, compression, replication, backup, archival and anticipated annual growth. Adequate capacity shall be provisioned for the complete contract period.	As per the RFP #1788963158, storage duration on the primary storage of the solution itself is mention for Cloud/SaaS/Hybrid to be 3 months, same is not clearly specified for VA & VM. Kindly confirm how long should the VA & VM solution retain the asset, vulnerability, logs, activities, historic trend etc. As per CERT-IN it must be 6 months. Kindly confirm if you wish the solution to retain this info on its own primary storage to be for 6 months or less.	Please refer addendum for revised clause
2139	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - VA-VM	VA-VM S.No. 9	Each scanning engine shall support web application security assessment together with traditional infrastructure vulnerability and configuration/compliance assessment. The solution shall identify vulnerabilities, missing patches, insecure configurations, and compliance deviations, and generate comprehensive reports containing risk severity, evidence of findings, affected assets, and remediation recommendations to support security governance, audit, and regulatory compliance.	While its possible to perform this via VA VM solution with additional WAS/DAST license, this will be a duplication of solution given you are already asking for seperate 'Application Security Testing Tool'. Hence, we request you to kindly move the 'Web application security assessment' from VA & VM requirements to DAST as this is a DAST requirement and may unnecessorily require to duplicate the licenses, solution and hardware.	No Change, Please be guided by the RFP
2140	Functional Compliance Sheet pp.48-51 (Appendix 1A)	Appendix 1A - VA-VM	VA-VM S.No. 36-52 and S.No. 61-77; S.No. 87 and S.No. 89	All technical compliances of VA-VM S.No. 36-52 and S.No. 61-77; S.No. 87 and S.No. 89	S.N 61-77 are likely duplicates of S.N 36 to 52 with minor changes. Request you to kindly review and confirm if this is intentional or typo. If not intentional, kindly remove duplicates to have the score calculated accordingly.	No Change, Please be guided by the RFP
2141	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 12	The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and failover capabilities.	VM solution is not an inline and always active solution.VM solutions across the industry do not have failovers similar to inline solutions such as firewalls. Hence, we request you to kindly consider the failover scenario as active - cold standby with documented backup-restore and a controlled switchover in place of automatic console failover. We request you to kindly update the clause as - The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and failover capabilities either automatically or using manual and controlled backup restore.	No Change, Please be guided by the RFP
2142	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 15	The proposed solution shall support integration with SIEM, SOAR, Threat Intelligence Platforms, NAC, and other security platforms through APIs or standard integration mechanisms.	Kindly share details (Vendor/Model/Version) of the SIEM, SOAR, TIP and NAC solution you would want to integrate with for us to identify the availablity of standard or API based integration and accordingly finalize the deployment efforts.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2143	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 16	The proposed solution shall integrate with Privileged Access Management (PAM) solutions for secure credential management during authenticated scans.	Kindly share details (Vendor/Model/Version) of the PAM solution you would want to integrate with for us to identify the availablity of integration and also identify the deployment efforts.	Bank is currently procuring PAM solution through separate RFP.
2144	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 17	The proposed solution shall integrate with IT Service Management (ITSM) and ticketing platforms for automated vulnerability tracking and remediation workflows.	Kindly share details (Vendor/Model/Version) of the ITSM solution you would want to integrate with for us to identify the availablity of standard or API based integration and accordingly finalize the deployment efforts.	ITSM - Manage Engine
2145	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 29	The proposed solution shall support vulnerability assessment and compliance reporting aligned with PCI DSS requirements.	We request you to kindly confirm whether you only require to perform PCI DSS internal scanning and reporting on-premises or you also require the PCI- ASV attestation. If Attestation is required, kindly share the exact asset count for which the attestation is needed and how many attestations are to be submitted within 1 year.	No Change, Please be guided by the RFP
2146	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 42	The solution shall support vulnerability assessment of VMware ESXi, Hyper-V, Nutanix AHV, Kubernetes, OpenShift and container platforms.	We request you to kindly confirm whether you need the OS and platform vulnerability assessment of these container solutions or you need a comprehensive container security solution with the ability to identity vulnerabilities of images, registries and their components. If you need comprehensive container security assessment, we request you to kinly move this required to CNAPP solution as its usually part of cloud security solutions and not VM solution.	No Change, Please be guided by the RFP
2147	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 45	The solution shall integrate with enterprise CMDB, ITSM, SIEM, SOAR, PAM and NAC platforms through secure REST APIs.	Kindly share details (Vendor/Model/Version) of the required solutions you would want to integrate with for us to identify the deployment efforts.	Please refer addendum for the revised clause Details shall be shared with successful bidder
2148	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 47	The solution shall support Multi-Factor Authentication (MFA), LDAP, Active Directory, SAML 2.0 and OpenID Connect authentication.	We request you to kindly remove the OpenID and update the clause as following - The solution shall support Multi-Factor Authentication (MFA via SAML and/or LDAP), LDAP, Active Directory, SAML 2.0.	No Change, Please be guided by the RFP
2149	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 48	The solution shall support secure encrypted communication using TLS 1.3 and cryptographic modules compliant with FIPS 140-3 or equivalent internationally recognized standards.	We request you to kindly allow the FIPS 140-2 or equivilent solution transitioning to FIPS 140-3 to participate and update the clause as following - The solution shall support secure encrypted communication using TLS 1.3 and cryptographic modules compliant with FIPS 140-2 or FIPS 140-3 or equivalent internationally recognized standards.	Please refer addendum for revised clause
2150	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 51	The solution shall identify internet-facing assets and continuously monitor externally exposed services.	We request you to kindly remove this clause as its an ASM(Attack Surface Management) requirements which is already asked separate service based solution of the RFP.	Please refer the addendum for revised clause
2151	Functional Compliance Sheet p.49 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 56	The solution shall support digitally signed and password-protected reports with configurable retention and archival.	We request you to kindly update the clause as following - The solution shall support password-protected reports with configurable retention and archival.	Please refer addendum for revised clause
2152	Functional Compliance Sheet p.49 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 60	The solution shall provide comprehensive REST APIs and webhook support for automation and integration with enterprise security platforms.	We request you to kindly update the clause as following - The solution shall provide comprehensive REST APIs or webhook support for automation and integration with enterprise security platforms.	Please refer addendum for revised clause
2153	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 87	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	We request you to kindly remove this clause from VM VM and move it to CTEM as this is a CTEM requirement, a solution that can be cloud/SaaS based. Given the data soveraginity and sensitivity of bank's vulnerabilities data, the platform is correctly requested to be on-prem which shall also be able to function without any internet connectivity. Hence, AI powering the on-prem application to achieve all the listed items is not viable. We request you to kindly remove this point and move it to CTEM.	Please refer the addendum for revised clause
2154	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 88	Unified, correlated findings intelligence. Every scanning engine — across web, API, network and host, cloud, containers, mobile, source code, device configuration and identity — reports into a single normalized findings model..	This is a CTEM requirement as VM solution won't perform VA of source code, identity etc. Kindly move this from VA VM to CTEM requirements.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2155	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 89	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	This is a duplicate of S.N. #87, kindly remove it.	Please refer the addendum for revised clause
2156	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 90	Mobile Application Security Testing: The proposed solution shall support static security analysis of Android and iOS mobile application packages, including APK/AAB and IPA formats, and shall provide security assessment mapped to recognized mobile application security standards and methodologies such as OWASP MASVS and MASTG.	This is not part of any VA/VM solution in industry and belongs to application security testing. We request you to kindly move this to 'Application Security Testing Tool'.	No Change, Please be guided by the RFP
2157	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 91	White-Label Reporting and Approval Workflow: The proposed solution shall support customizable/white-label security assessment reports, including organization-specific branding and configurable report content. The solution shall support role-based maker-checker workflow for report generation, review, approval, and controlled release of finalized reports.	We request you to kindly update the clause as following - White-Label Reporting and Approval Workflow: The proposed solution shall support customizable/white-label security assessment reports, including organization-specific branding and configurable report content. The solution shall support role-based access for report generation, review of the finalized reports.	Please refer addendum for the revised clause White-Label Reporting and Approval Workflow: The proposed solution shall support customizable/white-label security assessment reports, including organization-specific branding and configurable report content. The solution shall support role-based or maker-checker workflow for report generation, review, approval of finalized reports.
2158	92	7.18.1 Compute Infrastructure	10. Non-production:	10. Non-production: a) The non-production environments should have the same software and hardware setup as deployed in production environments meeting all RFP requirements.	While this clause suggests the hardware and software setup of non-prod to be same, "16.21 Annexure 21: Sizing/Volumetrics, Data Retention and Current Infrastructure" suggests the VM based solution to have minimum 10% size. Kindly confirm if the 10% requirement of non-production infra is for only licenses whereas the hardware specs are to be identical to prod or both the licenses as well as hardware/software specs to be 10% of the production infra. Also kindly confirm if the non-production is to be setup only at DC or DC as well as DR.	Please refer addendum for the revised clause
2159	Functional Compliance Sheet pp.47-51 (Appendix 1A)	Appendix 1A - VA-VM	TOTAL MARKS row and S.No. 1 to 94	TOTAL MARKS - 850	While the VA-VM section contains 94 scoreable clauses, each carrying Maximum Marks of 10, which totals 940 marks, whereas the TOTAL MARKS row of the section states 850. We request you to kindly publish the corrected total and confirm the marks allocated per clause, so that bidders can compute the Respective Solution Compliance required by the Appendix 1A summary sheet consistently.	Please refer addendum for the revised clause
2160	49	RFP - Scope of Work 7.3.10 Application security testing Tool	7.3.10.1 Modules, Architecture & Deployment:	Pt 2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Generally AST solutions are deployed with sole purpose of scanning the source code, web, api etc and does not have native 2FA capability, so request bank to remove this point. As an alternate as proposed in same point, proposed AST solution can be integrated with bank's existing MFA solution.	No Change, Please be guided by the RFP
2161	260	RFP - 16.21.2 Volumetrics- Solution-wise Requirements	12. Application Security Testing Tool	All the inline components of the solution must operate in high availability mode. In the event of any component failure, the system should automatically initiate failovers within seconds, ensuring uninterrupted functionality without requiring manual intervention.	Application Security Testing as a technology in general works at developemnt/pre-production/UAT stage only. And hence as a solution there is no need of high availability mode. Same has already been updated in this RFP (as solution is asked in standalone at both DC & DR). So, request bank to deleted this clause.	No Change, Please be guided by the RFP. The bidder must design the solution to fully comply with the RFP requirements, ensuring that in case of a failover, the system meets the defined SLA for availability, RTO, and RPO. The bidder is required to adhere to the deployment requirements outlined in the RFP when designing and proposing the solution architecture.
2162	42	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 3. The solution must be able to analyse a wide array of programming languages including Java,.Net, C/C++, Objective-C, Android, PHP, COBOL, Ruby, Swift, HTML 5, Scala, APEX, TypeScript, Go, Kotlin and ABAP etc but not limited to these alone	Considering the future requirements of AI in Secure Code Development and most of the development is moving towards AI generated code using AI supported languages. So it is very important for bank to have coverage around this as well and will recommend to incorporate AI supported languages like "R, Ada, Solidity, Bash, Groovy, Rust, Perl", but not limited to these alone.	No Change, Please be guided by the RFP
2163	42	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 24. Solution should support Machine learning and Analysis based on the archived results	ML capability is important, but it is very important to have coverage around AI based code as well. And will recommend bank to consider: The solution should have the capability to scan AI generated code. The solution should be able to integrate with AI coding agent via MCP	No Change, Please be guided by the RFP
2164	43	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 32. The solution should be able to support Composition Analysis: Identify the opens source components used in the application. Vulnerabilities & outdated version Licensing risk associated with the components	Bank is looking for Software composition analysis and asked for identifying the open source component and licensing risk. But this limited information is not enough for bank to secure themselves with rapidly increasing supply chain attacks and we will highly recommend to consider following as well: SCA system must catalogue open source components from Maven, NPM, and Nuget. SCA system has to be able to generate a Bill of Materials for an application. Solution should have the ability to continuously monitor the scanned components & notify if there are any zero day attacks without performing the rescan. Solution should Catalog, Store, and Audit SBOMs (both cycloneDx & SPDX) generated for in-house developed software applications and COTS applications.	No Change, Please be guided by the RFP
2165	137	12.1	Payment Terms-Product (Software) Cost	Milestone based and Quarterly in Arrears	As payment terms mentioned are milestone based and partially as Qarterly in Arrears, requesting the bank to make the payment terms as Annual in Advance.	No Change, Please be guided by the RFP
2166	138	12.2	OEM Services Cost		Our Software and Services go hand-in-hand and should be paid for together.	No Change, Please be guided by the RFP BOM

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2167	Page 2- Appendix 1A	1	CSP	Cloud must be hosted in India, and there should be no network and data sharing/replication to any datacenter/office outside the boundaries of India. Bound by Indian law, Indian IT Law, and the applicable regulations. No data in any circumstances should be shared/copied/transmitted without' s consent/written permission of the bank and it should be as per the Indian IT Law, RBI guidelines, bank policy & guidelines and other regulatory & statutory body in India	Our services do not gather any data from the client. We collect data related to the client which is already present on the Surface, deep & dark web. Also, many PSCs, Scheduled Commercial Banks in India are our clients	No Change, Please be guided by the RFP
2168	Page 2- Appendix 1A	18		18 The cloud infrastructure should have presence in at least 2 cities in India in different SEISMIC Zone		Please refer addendum for the revised clause
2169	Page 147 of RFP		Penalties- Services SLA	Non-detection or late detection - Rs. 1 Lakh each for non-detection or late detection of phishing site, anti-rogue, malware, social media, mobile app, etc. Point b to Point f -- Rs.5000/- for every hour beyond resolution time.	Requesting the bank to consider better penalty terms, consistent with market standards. These current panalties are very steep. Also, total penlty for a year should be capped at 5% of the yearly contract value.	No Change, Please be guided by the RFP
2170	95	7.19.2	4	The bidder shall run the existing SIEM on as-is/where-s basis for another 12 months from the date of Go-Live of the respective solutions.	Request Bank to confirm if the signoff against individual solutions will be provided as standalone solutions as and when individual solutions are deployed	The bank will provide individual sign-off for each respective solution.
2171	98		9 PROJECT TIMELINES	Overall Implementation period shall be 5 Months (Start Date is T0) for all solution & services	Request Bank to increase the overall implementation timeline to 12 months	No Change, Please be guided by the RFP
2172	98			The bidder shall submit the detailed Project Plan along with the proposal (mandatory) and subsequently within seven (7) days from T0 for the Bank's review and approval.	Request Bank to increase the timeline to 1 month for detailed project plan submission	No Change, Please be guided by the RFP
2173	159		14 TERMS AND CONDITIONS	14.1 Assignment & Subcontracting	Request Bank to allow outsourcing for the physical H&F support for Branches	No Change, Please be guided by the RFP
2174	159	14	14 TERMS AND CONDITIONS	14.1 Assignment & Subcontracting 1. The selected bidder shall not subcontract/JV/Consortium or permit anyone to perform anyof the work, service or other performance required under the contract (excluding Proposed OEM personnels). All bidder's personnel proposed for the bank shall be on bidder's Payroll. Bank will seek relevant documentation from the bidder to validate the same.	Request Bank to allow outsourcing for the physical H&F support for Branches	No Change, Please be guided by the RFP
2175				of the work, service or other performance required under the contract (excluding Proposed		Delete
2176				OEM personnels). All bidder's personnel proposed for the bank shall be on bidder's Payroll.		Delete
2177				Bank will seek relevant documentation from the bidder to validate the same.		Delete
2178				Acceptance criteria for successful implementation of various components of RFP	Request bank to share the acceptance criteria	No Change, Please be guided by the RFP. Details shall be shared with successful bidder on solution/case to case basis
2179			Page 157 Liquidated Damage	* Product Cost = Product License/Subscription Cost + Implementation + Configuration + Integration + Migration + Commissioning Cost. If the LD due to Implementation of the respective product cost/existing product cost reaches 25% of the implementation cost of the respective product/services, the bidder is required to replace the product/services.	LD for implementation shall be capped at 10% of the implementation/service component of the respective product, or such other mutually agreed cap. 25% clause should be removed due to interdependencies between implementation of various components.	No Change, Please be guided by the RFP
2180				If the LD due to Implementation of the respective product cost/existing product cost reaches 25% of the implementation cost of the respective product/services, the bidder is required to replace the product/services.		Delete
2181				product/services, the bidder is required to replace the product/services.		Delete
2182				7.3.7.1 – Point 6	The RFP requires matching threat intelligence against available security telemetry and assets. Kindly clarify the specific Bank security-telemetry sources and asset repositories that are expected to be integrated with the TIP for contextualization and relevance assessment.	Details shall be shared with successful bidder
2183				7.3.7.1 – Point 8	The RFP requires IOC lifecycle management covering creation, validation, enrichment, scoring, distribution, updating and expiration. Kindly clarify whether lifecycle management for all IOC types, including IP addresses, domains, URLs, hashes, email addresses and other supported indicators is expected.	No Change, Please be guided by the RFP
2184				7.3.7.1 – Point 9	The RFP requires configurable expiry periods based on indicator type, feed source or global retention policies. Kindly clarify the expected minimum retention period for threat intelligence and historical indicators.	No Change, Please be guided by the RFP
2185				7.3.7.2 – Point 4	The RFP requires integration with SIEM, SOAR, XDR, UEBA, NDR, CTEM, vulnerability management and other relevant security solutions. Kindly provide the OEM/product details and versions of the existing/proposed platforms with which the TIP is expected to integrate.	Bidder to proposed the solution as sort in the RFP
2186				7.3.7.2 – Point 7	The RFP requires custom threat-intelligence reports for significant security incidents and regulatory requirements. Kindly clarify the expected number/frequency of such custom reports and whether reports generated on an as-needed basis shall be acceptable.	No Change, Please be guided by the RFP
2187				7.3.7.2 – Point 8	The RFP requires periodic review, tuning and optimization of threat-intelligence sources, analytics and use cases. Kindly clarify the expected frequency of such reviews (monthly/quarterly or as required).	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2188				ASM – 7.4.3, Pg. 55–56	The RFP requires discovery of both internet-facing and internal assets. Kindly clarify whether it is expected to scan internal assets too.	No Change, Please be guided by the RFP
2189				Phishing Simulation – 7.4.4, Pg. 56	Kindly provide the approximate number of employees/users to be covered under the phishing simulation service and confirm whether the requirement includes multiple user groups/departments and privileged/high-risk users for campaign segmentation.	The Bidder shall size and quote the service based on the complete Bank user base. The Bank may conduct campaigns for the required users during the contract period. The Bidder shall ensure that the proposed service is scalable to meet the Bank's requirements.
2190	Page No.	Section	RFP Clause	Clause / Technical Specification	Bidder's Query	No Change, Please be guided by the RFP
2191	7	KEY INFORMATION	Security Deposit/Earnest Money deposit	Rs. 4.25 Crore (INR Four Crore and Twenty-Five Lakh Only) Note: - Bidders who are eligible for EMD (Earnest Money Deposit) exemption as per GeM General Terms and Conditions (GeM 4.0, Version 1.25, dated 14th July 2025, Page 19) are required to submit a Bid Security Declaration in lieu of EMD. Please refer to RFP, Annexure 4: Bid Security Declaration for the prescribed format. This declaration must be duly filled, signed, and submitted along with the bid documents by vendors seeking the waiver of EMD submission. Failure to submit the Bid Security Declaration (where applicable) will result in the bid being treated as non-responsive.	The RFP stipulates an EMD of ₹4.25 Crore and states that bidders eligible for EMD exemption as per GeM General Terms and Conditions (GeM 4.0, Version 1.25 dated 14th July 2025, Page 19) are required to submit a Bid Security Declaration in lieu of EMD. We request the Authority to kindly confirm whether bidders who are eligible for EMD exemption under the applicable GeM provisions as on the date mentioned above shall be permitted to participate in the tender without submitting the EMD of ₹4.25 Crore, subject to submission of the prescribed Bid Security Declaration as per Annexure 4 of the RFP. Further, kindly confirm that submission of the duly signed Bid Security Declaration shall be considered sufficient compliance with the EMD requirement for such eligible bidders and that their bids shall not be treated as non-responsive solely on account of non-submission of the EMD.	No Change, Please be guided by the RFP
2192	101	Eligibility Evaluation Criteria	10.2, Eligibility Evaluation Criteria	The bidder should have a minimum average turnover of INR 500 crore per annum in India during the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth. Note – In case of MSMEs only, the turnover may be relaxed subject to meeting the quality and technical speci cations.	Request PSB to kindly give relaxation on this clause. Turnover of 500 crore is very high considering the size of the project	No Change, Please be guided by the RFP
2193	192	Eligibility Evaluation Criteria	10.2, Eligibility Evaluation Criteria	Proposed OEM SIEM solution ≥30,000 EPS or 1.2 TB/day successfully implemented and under management/maintenance in at least one BFSI in India; also successfully implemented on cloud in one India deployment. Client PO/WO/Contract + client supporting document + OEM self-declaration	OEM SIEM solution ≥30,000 EPS or 1.2 TB/day successfully implemented and under management/maintenance in at least one BFSI in India; also successfully implemented on cloud or Hybrid in one organisation Globally	Please refer addendum for revised clause.
2194			7.2.1	SIEM, SOAR and UEBA are explicitly required as Cloud (SaaS) + Hybrid solutions, not pure on-premises deployments.	SIEM, SOAR and UEBA are required as Cloud (SaaS) or Hybrid Solutions Deployment	Please refer addendum for the revised deployment architecture
2195	136	12.4	Payment Terms	Annually in Advance: Upon submission of a Bank Guarantee equivalent to 110% of the annual subscription/Annual technical cost of the respective product, valid for the applicable subscription period; or Quarterly in Arrears	As per prevailing industry/OEM policy, the ATC/subscription charges are generally payable in advance. However, PSB has stipulated payment on a quarterly-in-arrears basis. This payment structure will adversely impact the bidder's cash flow and may result in additional financing costs, which would ultimately increase the overall bid price. Alternatively, if a bidder opts for advance payment by providing an additional PBG, the associated financial and administrative costs would again increase the project cost. Moreover, PSB is already requiring a PBG under the tender conditions. In view of the above, we request the Department to kindly reconsider and remove the Advance BG clause. This will reduce the additional financial burden on bidders, avoid unnecessary financing costs, and encourage wider participation, thereby making the bid more competitive and cost-effective for PSB. We request the Department to kindly consider this amendment in the interest of healthy competition and optimal pricing.	No Change, Please be guided by the RFP
2196			Price Bid Formet	Product License Cost	We request the Department to kindly clarify where the Bidder should quote the price for the cloud-based license/subscription, as OEMs generally offer such licenses on a monthly, quarterly, or annual subscription basis. Further, the RFP specifies a warranty period of 3 years. In this regard, kindly clarify whether the Bidder is required to quote the complete 3-year license/subscription cost upfront under the Product License Cost Sheet, or whether the license cost is to be quoted based on the OEM's applicable subscription billing cycle. Clear guidance on the above will help bidders ensure uniformity in their commercial quotations and avoid any ambiguity in the evaluation of the bids.	The pricing shall be provided in the two separate sheets provided in the BOM/pricing template: Product License Cost: The bidder shall quote the applicable one-time perpetual license cost or initial subscription cost, as applicable, for the respective products/solutions. The relevant product/license details shall be provided in this sheet. ATS / Annual Subscription Cost: The bidder shall quote the applicable Annual Technical Support (ATS) / Annual Subscription Renewal Cost in the sheet provided for Y1 to Y5, post Go-Live. The bidder shall clearly identify the applicable licensing model (Perpetual/Subscription) for each product/solution and ensure that there is no duplication between the Product License Cost and ATS/Annual Subscription Cost. The BOM/pricing format remains unchanged.
2197	21	PBG	6.11 sub-clause 9	Cure period mentioned as 30 days	cure period of 30 60 days would be viable.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2198	141	Service Levels & Penalties	Clause 13 sub clause 13.1(8)	Failure to provide support services in accordance with the SLA requirements, including the required support coverage and service quality specified in this RFP, may result in bank levying penalty, termination of the contract, or any other action deemed appropriate by the Bank, without prejudice to its other contractual rights and remedies.	We propose to modify the clause:- Failure to provide support services in accordance with the SLA requirements, including the required support coverage and service quality specified in this RFP, the Bidder be provided with a cure period of 30 days to remedy the defects/deficiency. However, if the Bidder fails to rectify the defects/deficiency within the cure period, then the Bank may levy penalty at the rate of ___ (of the total contract value), termination of the contract, or any other action deemed appropriate by the Bank, without prejudice to its other contractual rights and remedies.	No Change, Please be guided by the RFP
2199	159	Terms and Conditions	Clause 14 sub clause 14.1(2)	If the Bank undergoes a merger, amalgamation, takeover, consolidation, reconstruction, change of ownership, etc., this tender shall be assigned to the new entity, and such an act shall not affect the rights of the Agency under this tender.	We propose to modify the clause:- If the Bank undergoes a merger, amalgamation, takeover, consolidation, reconstruction, change of ownership, etc., this tender shall be assigned to the new entity, and such an act shall not affect the rights of the Bidder under this tender. Also, the new entity shall be bound by the terms of the SLA, NDA and all the agreements/contracts entered into by and betweeen the Bank and the Bidder, as if the same has been entered into by and between the new entity and the Bidder.	No Change, Please be guided by the RFP
2200	159	Terms and Conditions	Clause 14 sub clause 14.2	The bank reserves the right, at the time of award of contract and/or during the currency of the contract, to increase or decrease the quantity of goods, licenses, subscriptions, appliances, equipment, services, implementation effort, support services, or any line item covered under the contract by up to twenty-five percent (25%) of the quantities specified in the RFP/Contract, without any change in the unit prices, terms and conditions, technical specifications, delivery schedule, warranty obligations, support commitments, or any other contractual conditions.	We propose to modify the clause:- The bank reserves the right, at the time of award of contract and/or during the currency of the contract, to increase or decrease the quantity of goods, licenses, subscriptions, appliances, equipment, services, implementation effort, support services, or any line item covered under the contract by up to ten percent (10%) of the quantities specified in the RFP/Contract, without any change in the unit prices, terms and conditions, technical specifications, delivery schedule, warranty obligations, support commitments, or any other contractual conditions. Also, the Bank will notify the Bidder by a ten days (10) prior written notice before changing the quantities of any of the above listed services/goods/materials.	No Change, Please be guided by the RFP
2201			-	Legal Query	We reccomend to add below clause under the RFP:- Termination by the Bidder for breach:- In the event BSNL materially breaches this definitive Agreement or any statement of work, which breach is not cured within thirty (30) days after written notice specifying the breach is given to the BSNL, the Contractor may terminate this defenitive Agreement or any portion thereof or the applicable statement of work by giving written notice to the BSNL.	No Change, Please be guided by the RFP
2202			-	Legal Query	We recommend to incorporate a new clause under the RFP, which shall be mutually beneficial and significant in the context of business engagements Non-Solicitation:- During the Term of this definitive Agreement and for a period of one year thereafter, neither Party shall (either directly or indirectly through a third party) solicit to employ, cause to be solicited for the purpose of employment to any employee/s (including the employees who have been exposed or introduced to other Party during initial discussion between Parties or engaged to provide/perform the services under any definitive agreement entered between Parties) of the other Party or aid any third person to do so, without the specific written consent of the other Party. The said restriction shall also apply to each Party's affiliates, agents, vendors, contractors, and any third parties with whom such Party has a relationship (collectively, "Representatives"). Parties agree that Representatives are equally restricted from poaching or soliciting or inducing any employees of other Party to leave their employment or engagement with such other Party.	No Change, Please be guided by the RFP
2203			Functional Specification	The proposed solution shall support dynamic log parsing and normalization upon ingestion. In cases where historical security telemetry must be re-parsed, re-processed, or re-modeled using updated parsing rules or processing logic, the platform shall provide high-speed, cloud-native mechanisms to re-process retained historical telemetry using the updated parsing and processing logic, without impacting active SOC performance, availability, or operational detection capabilities.	The proposed solution shall support dynamic log parsing and normalization upon ingestion. In cases where historical security telemetry must be re-parsed, re-processed, or re-modeled using updated parsing rules or processing logic, the platform shall provide high-speed, cloud-native/hybrid mechanisms to re-process retained historical telemetry using the updated parsing and processing logic, without impacting active SOC performance, availability, or operational detection capabilities.	No Change, Please be guided by the RFP
2204			Functional Specification	The proposed solution shall be scalable and shall provide a cloud-native, highly available architecture with built-in redundancy and service continuity. The solution shall provide continuous security monitoring through cloud-native high availability and disaster recovery capabilities, with a minimum uptime commitment of 99.9%	The proposed solution shall be scalable and shall provide a cloud-native/hybrid highly available architecture with built-in redundancy and service continuity. The solution shall provide continuous security monitoring through cloud-native/hybrid high availability and disaster recovery capabilities, with guaranteed High availability/Redendency	No Change, Please be guided by the RFP
2205			Functional Specification	The proposed solution shall provide cloud-native high availability and redundancy mechanisms to tolerate failures of underlying infrastructure components without disruption to security monitoring and operational capabilities. The solution shall provide automated failover and service continuity within the cloud environment through the CSP's native availability and resiliency capabilities	The proposed solution shall provide cloud-native/hybrid high availability and redundancy mechanisms to tolerate failures of underlying infrastructure components without disruption to security monitoring and operational capabilities. The solution shall provide automated failover and service continuity within the cloud environment through the CSP's native or Hybrid solution's availability and resiliency capabilities	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2206			Functional Specification	The proposed cloud-based solution shall support flexible data representation and analysis by enabling multiple views, schema interpretations, and query-time transformations of the same collected data without requiring redundant data storage or unnecessary reprocessing. The cloud platform shall support creation of customized searches, dashboards, and reports based on business and security monitoring requirements.	The proposed cloud-based/hybrid solution shall support flexible data representation and analysis by enabling multiple views, schema interpretations, and query-time transformations of the same collected data without requiring redundant data storage or unnecessary reprocessing. The cloud/hybrid platform shall support creation of customized searches, dashboards, and reports based on business and security monitoring requirements.	No Change, Please be guided by the RFP
2207		NDR	Functional Specification	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	The proposed solution shall feature a cloud-native SaaS/Hybrid console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud/hybrid architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	Please refer Addendum for revised clause
2208			Functional Specification	The proposed cloud-delivered solution shall provide appropriate encryption, tenant isolation, secure authentication, MFA, RBAC, audit logging and protection of Bank security data in accordance with the applicable service architecture and SLA.	The proposed cloud-delivered/hybrid solution shall provide appropriate encryption, tenant isolation, secure authentication, MFA, RBAC, audit logging and protection of Bank security data in accordance with the applicable service architecture and SLA.	No Change, Please be guided by the RFP
2209	45	RFP - Scope of Work 7.3.5 Network detection and response (NDR)	7.3.5.1 Modules, Architecture & Deployment:	Pt 2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Generally NDR solutions are deployed with sole purpose of doing network analysis, threat detection & response and does not have native 2FA capability, so request bank to remove this point. As an alternate as proposed in same point, proposed NDR solution can be integrated with bank's existing MFA solution.	Please refer addendum for the revised clause
2210	49	RFP - Scope of Work 7.3.10 Application security testing Tool	7.3.10.1 Modules, Architecture & Deployment:	Pt 2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Generally AST solutions are deployed with sole purpose of scanning the source code, web, api etc and does not have native 2FA capability, so request bank to remove this point. As an alternate as proposed in same point, proposed AST solution can be integrated with bank's existing MFA solution.	No Change, Please be guided by the RFP
2211	110	RFP - 10.2 Eligibility Evaluation Criteria	OEM Evaluation Criteria	Pt 19. The proposed OEM SIEM Solution with a minimum capacity of 30,000 EPS or 1.2 TB/day shall have been successfully implemented on cloud in one (1) in India.	For wider participation, we request bank to amend the clause as: The proposed OEM SIEM Solution with a minimum capacity of 5,000 EPS or.2 TB/day shall have been successfully implemented on cloud in any one (1) Govt/PSU customer in India. OR The proposed OEM SIEM Solution with a minimum capacity of 10,000 EPS or.4 TB/day shall have been successfully implemented on cloud in one (1) in India.	Please refer addendum for revised clause.
2212	112	RFP - 10.2 Eligibility Evaluation Criteria	OEM Evaluation Criteria	Pt 20. The proposed OEM solution should have been implemented in at least one BFSI is to be submitted for the following solutions: NDR	For wider participation, we request bank to amend the clause as: The proposed OEM solution should have been implemented in at least one BFSI / Govt is to be submitted for the following solutions: NDR	Please refer addendum for the revised clause
2213	260	RFP - 16.21.2 Volumetrics- Solution-wise Requirements	12. Application Security Testing Tool	All the inline components of the solution must operate in high availability mode. In the event of any component failure, the system should automatically initiate failovers within seconds, ensuring uninterrupted functionality without requiring manual intervention.	Application Security Testing as a technology in general works at developemnt/pre-production/UAT stage only. And hence as a solution there is no need of high availability mode. Same has already been updated in this RFP (as solution is asked in standalone at both DC & DR). So, request bank to deleted this clause.	No Change, Please be guided by the RFP. The bidder must design the solution to fully comply with the RFP requirements, ensuring that in case of a failover, the system meets the defined SLA for availability, RTO, and RPO. The bidder is required to adhere to the deployment requirements outlined in the RFP when designing and proposing the solution architecture.
2214	40	APPENDIX 1A Functional Compliance Sheet (Solutions)	Network Detection & Response (NDR)	Pt 13. The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	As bank has asked for on-premise solution for NDR, on the contrary, this clause asks for cloud-native SAAS ask. So, we kindly request bank to delete this clause.	Please refer Addendum for revised clause
2215	42	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 3. The solution must be able to analyse a wide array of programming languages including Java,.Net, C/C++, Objective-C, Android, PHP, COBOL, Ruby, Swift, HTML 5, Scala, APEX, TypeScript, Go, Kotlin and ABAP etc but not limited to these alone	Considering the future requirements of AI in Secure Code Development and most of the development is moving towards AI generated code using AI supported languages. So it is very important for bank to have coverage around this as well and will recommend to incorporate AI supported languages like "R, Ada, Solidity, Bash, Groovy, Rust, Perl", but not limited to these alone.	No Change, Please be guided by the RFP
2216	42	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 24. Solution should support Machine learning and Analysis based on the archived results	ML capability is important, but it is very important to have coverage around AI based code as well. And will recommend bank to consider: The solution should have the capability to scan AI generated code. The solution should be able to integrate with AI coding agent via MCP	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2217	43	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 32. The solution should be able to support Composition Analysis: Identify the opens source components used in the application. Vulnerabilities & outdated version Licensing risk associated with the components	Bank is looking for Software composition analysis and asked for identifying the open source component and licensing risk. But this limited information is not enough for bank to secure themselves with rapidly increasing supply chain attacks and we will highly recommend to consider following as well: SCA system must catalogue open source components from Maven, NPM, and Nuget. SCA system has to be able to generate a Bill of Materials for an application. Solution should have the ability to continuously monitor the scanned components & notify if there are any zero day attacks without performing the rescan. Solution should Catalog, Store, and Audit SBOMs (both cycloneDx & SPDX) generated for in-house developed software applications and COTS applications.	No Change, Please be guided by the RFP
2218		16.21.2	7.3.11	VMs (VPCs) Counts - 20	Which cloud platform is currently in use or planned to be used (AWS, Azure, GCP, OCI, VMware, etc.)?	Details shall be shared with successful bidder
2219		16.21.2	7.3.11	VMs (VPCs) Counts - 20	How many cloud accounts, subscriptions, or projects are in-scope?	Details shall be discussed with the successful bidder
2220		16.21.2	7.3.11	VMs (VPCs) Counts - 20	Are there any databases (PaaS), storage buckets, data disks (disks attached to VMs, other than OS disks), or special PaaS services in use? Please share the count for each.	No Change, Please be guided by the RFP
2221		16.21.2	7.3.11	VMs (VPCs) Counts - 20	Are there any AI-related services hosted on the cloud platform? If yes, please specify.	No Change, Please be guided by the RFP
2222		16.21.2	7.3.11	VMs (VPCs) Counts - 20	VMs count mentioned in the RFP is the final count, or are additional VMs expected to be added?	Details shall be discussed with succesfull bidder
2223		16.21.2	7.3.11	VMs (VPCs) Counts - 20	Do you operate any serverless functions (e.g., AWS Lambda, Azure Functions, Google Cloud Functions), or are any planned? Please share the count.	Details shall be shared with successful bidder
2224			7.3.13	20 VPCs/Vnets VMs Count - 100	Please share the breakup of virtual machines by OS (Windows/Linux). VMs count mentioned in the RFP is the final count, or are additional VMs expected to be added?	Details shall be shared with the successful bidder
2225			7.3.13	20 VPCs/Vnets VMs Count - 100	Are there any container clusters (e.g., Kubernetes, ECS, AKS, GKE) and nodes currently active or planned? Please share the count.	No Change, Please be guided by the RFP
2226			7.3.13	20 VPCs/Vnets VMs Count - 100	Are there any serverless containers (e.g., EKS/ECS on Fargate, SageMaker) in use or planned? Please share the count.	No Change, Please be guided by the RFP
2227			7.3.13	20 VPCs/Vnets VMs Count - 100	Will private cloud or on-premises virtualization environments (e.g., VMware/ESXi, Hyper-V, bare metal, OpenStack) also be covered under CWPP, or is the scope limited to public cloud (Azure/AWS/OCI/GCP)? Please confirm.	No Change, Please be guided by the RFP, refer section 7.3.13, which states "The Bank intends to implement CWPP to provide comprehensive security for cloud workloads deployed across public cloud, private cloud, hybrid cloud, and on-premises environments."
2228			7.3.12	20 VPCs/Vnets VMs Count - 100	Which code repository/VCS tools are currently in use (e.g., GitHub, GitLab, Bitbucket)? Please share the details and count.	Details shall be shared with the successful bidder.
2229			7.3.12	20 VPCs/Vnets VMs Count - 100	Which identity provider is currently in use (e.g., Microsoft Entra ID, Google Workspace, Okta)? Please share the details.	Details shall be shared with successful bidder
2230			7.3.12	20 VPCs/Vnets VMs Count - 100	How many users have been provisioned with cloud accounts?	Details shall be discussed with the successful bidder
2231			7.3.12	20 VPCs/Vnets VMs Count - 100	Are there any CI/CD pipelines in use? If yes, please share the count that needs to be integrated with CNAPP for security scanning.	Details shall be discussed with the successful bidder
2232			7.3.12	20 VPCs/Vnets VMs Count - 100	Are there any IaC tools (e.g., Terraform, ARM, Bicep) currently in use? Please specify.	No Change, Please be guided by the RFP
2233			7.3.12	20 VPCs/Vnets VMs Count - 100	Is there any secrets management tool in use (e.g., Azure Key Vault, AWS Secrets Manager)? Please specify.	Details shall be shared with successful bidder
2234			7.3.12	20 VPCs/Vnets VMs Count - 100	How many applications are running on the cloud VMs, and how many APIs are internet-exposed? VMs count mentioned in the RFP is the final count, or are additional VMs expected to be added?	Details shall be discussed with the successful bidder
2235					What is the MFA solution currently in use?	Bank is in the process of procuring the MFA tool
2236					Are there any existing CNAPP, CSPM, or CWPP tools currently in use? If yes, please specify.	Bidder is required to provide the same as a part of the RFP
2237					Is there any endpoint protection agent (MDE, CrowdStrike etc.) currently running on the cloud VMs? If yes, will it be replaced by the proposed CWPP solution, or will both coexist?	No Change, Please be guided by the RFP. Details shall be shared with the successful
2238		7.3.4	Extended Detection and Response (XDR) 7.3.4		Which endpoint security product is currently deployed (OEM, version, deployment model) and is coexistence with the proposed XDR mandatory?	Details shall be shared with successful bidder
2239			Extended Detection and Response (XDR) 7.3.4		What percentage of endpoints have administrative restrictions that would prevent deployment of additional sensors?	The bidder shall size and propose the solution based on the endpoint scope specified in the RFP.
2240			Extended Detection and Response (XDR) 7.3.4		What is the expected telemetry retention period for hot, warm and archived data?	Retention shall be as specified in the RFP and data retention requirements. The bidder shall propose the required architecture accordingly.
2241			Extended Detection and Response (XDR) 7.3.4		Are there any restrictions on OEM cloud connectivity?	No Change, Please be guided by the RFP
2242			Extended Detection and Response (XDR) 7.3.4		Is active-active deployment required between DC and DR?	The Bidder proposed solution should comply with the bank's defined SLA
2243			Extended Detection and Response (XDR) 7.3.4		Will the Bank provide a pilot environment before enterprise rollout?	Bidder to propose and factor any component required to meet the scope & terms of the RFP
2244			Extended Detection and Response (XDR) 7.3.4		Are existing detection rules, use cases and incident data required to be migrated into the new XDR platform?	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2245			Extended Detection and Response (XDR) 7.3.4		What is the EPM tool that is in place which will be used for the agent deployment?	Bidder as a part of holistic solution required to factored in "TIF" i.e commercial as well as OSINT and same is to be integrated with proposed "TIP"
2246		7.4.1	Breach Attack & Simulation 7.4.1	Continuous validation of security controls against known attack techniques	Please clarify the expected frequency of BAS execution (continuous, daily, weekly, monthly, or quarterly) and whether simulations are required to run autonomously.	No Change, Please be guided by the RFP. Details shall be shared with successful bidder
2247			Breach Attack & Simulation 7.4.1	Assessment across network, endpoint, identity, application, cloud, and hybrid environments	Kindly provide the approximate scope, asset count, and technology landscape (endpoints, servers, cloud workloads, applications, identity platforms, etc.) to be covered under BAS.	Details shall be discussed with succesfull bidder
2248			Breach Attack & Simulation 7.4.1	Assessment of security control effectiveness	Please confirm the list of security solutions currently deployed (EDR/XDR, SIEM, SOAR, Email Security, Firewall, IPS, IAM, WAF, CASB, etc.) that need to be validated through BAS.	BAS shall cover the security controls and technology landscape relevant to the Bank. Detailed integration/validation scope shall be finalized during implementation.
2249			Breach Attack & Simulation 7.4.1	Mapping of attack scenarios to MITRE ATT&CK	Is the Bank expecting coverage against the complete MITRE ATT&CK framework or only selected tactics, techniques, and procedures (TTPs)?	No Change, Please be guided by the RFP
2250			Breach Attack & Simulation 7.4.1	Validation of detection, prevention, and response capabilities	Please clarify whether the scope includes validation of SOC analyst response workflows and incident response processes in addition to technical control validation.	No Change, Please be guided by the RFP
2251			Breach Attack & Simulation 7.4.1	Identification of control gaps, security weaknesses, and attack paths	Is attack path validation expected only within individual domains or across hybrid attack chains covering on-premises, cloud, identity, and endpoint environments?	No Change, Please be guided by the RFP
2252			Breach Attack & Simulation 7.4.1	AI-assisted attack path analysis and control gap identification	Please clarify whether the Bank mandates a specific BAS platform or vendor solution with AI capabilities, or if equivalent industry-recognized solutions are acceptable.	No Change, Please be guided by the RFP
2253			Breach Attack & Simulation 7.4.1	Executive, operational, and technical reporting	Kindly provide the expected reporting frequency and reporting format requirements for Executive, Operational, and Technical reports.	No Change, Please be guided by the RFP
2254			Breach Attack & Simulation 7.4.1	Risk-based prioritization and remediation recommendations	Is the bidder expected to provide remediation validation/retesting after implementation of recommendations, and if so, what is the expected frequency?	No Change, Please be guided by the RFP
2255			Breach Attack & Simulation 7.4.1	Continuous BAS services	Please clarify whether the Bank currently has an existing Breach Attack & Simulation (BAS) platform deployed. If yes, kindly provide details of the solution/vendor and the expected scope of services to be delivered on the existing platform. If not, is the bidder expected to provide, implement, and manage the BAS solution along with the required licenses/subscriptions as part of the engagement?	No Change, Please be guided by the RFP
2256			Breach Attack & Simulation 7.4.1	Continuous validation	Please confirm whether production environment testing is permitted and identify any restrictions regarding business-critical systems.	Details shall be discussed and deliberated with the successful bidder
2257			Breach Attack & Simulation 7.4.1	Scope of attack techniques	Are controlled malware, ransomware, phishing, credential abuse, lateral movement, and privilege escalation simulations expected as part of the BAS program?	No Change, Please be guided by the RFP
2258			Breach Attack & Simulation 7.4.1	Coverage of cloud and hybrid environments	Kindly specify the cloud platforms in scope (Azure, AWS, GCP, Private Cloud) and the estimated workloads requiring BAS coverage.	Details shall be shared with the successful bidder
2259		7.4.2	Continuous Automated Red Teaming Services 7.4.2	Continuous automated Red Team exercises	Please clarify the expected frequency of Continuous Automated Red Teaming (CART) activities and whether attack simulations are required to run continuously or at predefined intervals.	No Change, Please be guided by the RFP
2260			Continuous Automated Red Teaming Services 7.4.2	Adversary emulation using realistic attack scenarios	Kindly provide the threat scenarios, threat actor profiles, or threat intelligence frameworks that should be used for adversary emulation.	Details shall be discussed and deliberated with the successful bidder
2261			Continuous Automated Red Teaming Services 7.4.2	Testing of people, processes, and technology	Please clarify whether the scope includes validation of people-centric controls such as phishing simulations and SOC analyst response testing, in addition to technical controls.	No Change, Please be guided by the RFP
2262			Continuous Automated Red Teaming Services 7.4.2	Validation of SOC detection and incident response capabilities	Kindly confirm whether the bidder is expected to coordinate directly with the Bank's SOC team during simulations and whether blue team awareness is permitted.	Bidder who would also be managing the SOC
2263			Continuous Automated Red Teaming Services 7.4.2	Assessment of identity, network, cloud, application, endpoint, and AI attack vectors	Please provide the approximate number of in-scope assets and technology landscape across on-premises, cloud, identity, applications, endpoints, and AI systems.	Detailed asset information shall be shared with the selected bidder on a need-to-know basis during implementation
2264			Continuous Automated Red Teaming Services 7.4.2	AI attack vectors	Kindly clarify the AI platforms, AI-enabled applications, LLM deployments, or AI services expected to be assessed as part of the engagement.	Detailed information shall be provided to the selected bidder as required.
2265			Continuous Automated Red Teaming Services 7.4.2	Attack path analysis and privilege escalation validation	Please confirm whether attack path validation is expected to include Active Directory, Entra ID/Azure AD, cloud environments, and hybrid identity architectures.	No Change, Please be guided by the RFP
2266			Continuous Automated Red Teaming Services 7.4.2	Recommendations for improving cyber resilience	Is the bidder expected to perform validation or retesting after remediation activities have been completed by the Bank?	Retesting shall be performed as required by the Bank and within the scope of services defined in the RFP.
2267			Continuous Automated Red Teaming Services 7.4.2	AI-assisted automated attack simulation and attack path analysis	Please clarify the Bank's expectations regarding the AI-assisted attack simulation capability. Specifically, whether the requirement is limited to AI-driven attack path discovery, control gap identification, and risk prioritization, or whether the solution is expected to autonomously emulate end-to-end adversary attack chains (e.g., reconnaissance, external attack simulation, initial access, privilege escalation, lateral movement, and objective execution). Additionally, kindly clarify the expected scope of AI-enabled validation across external, internal, cloud, identity, application, and AI-specific attack scenarios.	The proposed solution shall meet the AI-assisted attack simulation and attack-path analysis requirements specified in the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2268			Continuous Automated Red Teaming Services 7.4.2	Continuous Automated Red Teaming (CART) capabilities	Please clarify whether the Bank currently has an existing Continuous Automated Red Teaming (CART) platform deployed. If yes, kindly provide details of the solution/vendor and the scope of services expected on the existing platform. If not, is the bidder expected to provide, implement, operate, and license the CART solution as part of the engagement?	Details shall be shared with the successful bidder
2269			Continuous Automated Red Teaming Services 7.4.2	Simulate real-world cyberattacks	Kindly confirm whether production environments are within scope and specify any restrictions on business-critical applications or systems during attack simulations.	Production testing shall require prior approval from the Bank and shall be conducted under approved rules of engagement and change/security controls. Detailed information shall be provided to the selected bidder as required.
2270			Continuous Automated Red Teaming Services 7.4.2	Real-world cyberattacks against the organization's attack surface	Are simulations involving phishing, credential harvesting, lateral movement, privilege escalation, ransomware behavior, data exfiltration, cloud compromise, and insider threat scenarios expected as part of the engagement?	Controlled simulation of relevant attack scenarios should be performed as sought in the RFP
2271			Continuous Automated Red Teaming Services 7.4.2	Validate effectiveness of existing security controls	Please provide details of security controls/tools currently deployed (SIEM, SOAR, EDR/XDR, IAM, PAM, Email Security, DLP, WAF, CSPM, CNAPP, etc.) that are expected to be validated through CART activities.	Relevant security controls within the Bank's in-scope environment shall be validated. Detailed technology inventory shall be shared with the selected bidder on a need-to-know basis.
2272			Continuous Automated Red Teaming Services 7.4.2	Continuous monitoring and cyber resilience assessment	Kindly provide the expected reporting frequency, deliverables, KPIs, and SLAs for the Continuous Automated Red Teaming service.	No Change, Please be guided by the RFP
2273			Continuous Automated Red Teaming Services 7.4.2	Continuous Automated Red Teaming capabilities	Please clarify whether the Bank expects agent-based deployment, agentless deployment, or both approaches for conducting automated Red Team activities across the environment.	Bidder to design the approach and methodology
2274			Continuous Automated Red Teaming Services 7.4.2	Continuous Automated Red Teaming	Since automated Red Teaming capabilities may overlap with Breach Attack & Simulation (BAS) use cases, kindly clarify the expected distinction between the BAS and CART workstreams, including the scope, objectives, reporting requirements, and technology expectations for each service.	Bidder to comply with the FRS provided in the RFP
2275		7.3.7	Threat Intelligence Platform 7.3.7	TIP to aggregate intelligence from multiple sources and perform IOC lifecycle management	Please confirm whether the Bank expects commercial third-party intelligence feeds to be included within the TIP subscription or procured separately by the Bank.	Bidder as a part of holistic solution required to factored in "TIF" i.e commercial as well as OSINT and same is to be integrated with proposed "TIP"
2276		7.3.7.2	Threat Intelligence Platform	Custom threat intelligence reports for significant incidents	Please clarify the expected frequency and maximum number of ad-hoc/custom intelligence reports per year.	No Change, Please be guided by the RFP.
2277		7.4.3	Attack Surface Management	Discovery of domains, cloud assets, APIs and certificates	Please confirm the expected volume of domains, IP ranges, cloud subscriptions/accounts and external applications to be monitored.	Details of existing solutions, where applicable, shall be shared with the selected bidder on a need-to-know basis.
2278		7.4.5	Anti-Phishing	Detection and monitoring of phishing websites, domains, emails and URLs	Please confirm if there is an existing brand protection and monitoring solution implemented.	Details of existing solutions, where applicable, shall be shared with the selected bidder on a need-to-know basis.
2279		7.4.5	Anti-Phishing	Detection and monitoring of phishing websites, domains, emails and URLs	Please confirm whether takedown of phishing sites/domains is part of the anti-phishing service scope or only detection and reporting.	No Change, Please be guided by the RFP
2280		7.4.5 / SLA	Anti-Phishing Service & SLA	24x7 monitoring and detection effectiveness requirements	Please clarify the methodology that will be used by the Bank to measure anti-phishing detection effectiveness and associated SLA compliance.	Please refer to the relevant Addendum for updated specfications
2281		7.4.9	Brand Protection & Monitoring	Continuous monitoring for brand impersonation and fraudulent activities	Please provide the number of brands, sub-brands, trademarks and business units to be monitored under the service.	No Change, Please be guided by the RFP
2282		7.4.9	Brand Protection & Monitoring	Monitoring of domains, mobile apps, social media and executive impersonation	Kindly specify the number of executives, social media accounts and official mobile applications to be covered.	No Change, Please be guided by the RFP
2283		7.4.9	Brand Protection & Monitoring	Continuous monitoring and prioritization of threats	Kindly clarify the expected SLA for takedown completion where third-party registrar/platform response is outside bidder control.	No Change, Please be guided by the RFP
2284		7.4.6	Dark Web Monitoring	Monitoring employee and executive exposure	Kindly confirm the approximate number of email domains, executive accounts and privileged identities to be monitored.	Detailed domain and identity information shall be provided to the selected bidder on a need-to-know basis
2285		7.4.6	Dark Web Monitoring	Timely notification of critical or high-risk exposures	Kindly confirm the required notification SLA for critical findings and whether 24x7 analyst support is expected.	Notification shall be provided within the applicable incident/SLA timelines specified in the RFP. 24x7 monitoring/support shall be provided
2286		7.4.7	Threat Intelligence Feed	IOC, IOA, malware, ransomware and vulnerability intelligence	Please clarify whether the Bank expects commercial premium intelligence feeds or standard OEM-curated feeds.	No Change, Please be guided by the RFP
2287		7.4.7	Threat Intelligence Feed	Daily updates and monthly reporting	Kindly clarify whether automated feed integration into existing SIEM/TIP is mandatory or optional.	No Change, Please be guided by the RFP
2288		7.3.5	Network detection and response (NDR)	The Bank requires the solution to provide comprehensive Network Detection and Response (NDR) capabilities across its network infrastructure. The solution shall provide continuous network visibility, traffic analysis, threat detection, behavioral analysis, anomaly detection, investigation, threat hunting, network forensics and response capabilities. The solution shall support detection of advanced network threats including command -and-control activity, lateral movement, reconnaissance, data exfiltration, malicious communications and other sophisticated attacks. The NDR solution shall support integration with the Bank's existing network security environment, SIEM, SOAR, UEBA, NDR, XDR, firewall, ITSM and other relevant security solutions, as applicable.	As per the RFP deployment is On-Premise deployment only, can the Bidder propose a SaaS-based / Cloud-hosted NDR solution as an alternative. We want to propose SaaS based please help	Please refer addendum for revised clause
2289			Network detection and response (NDR)		Network Scope & Scale: Kindly share the total number of network segments, sites/branches, data centers, and DR locations where NDR visibility and monitoring is required, along with the total network bandwidth (in Gbps) to be monitored at each location.	Please refer addendum for revised clause
2290			Network detection and response (NDR)		Traffic Volume: What is the average and peak network traffic volume (North-South and East-West) across the Bank's infrastructure that needs to be analyzed by the NDR solution? Please specify in terms of EPS/FPS or Gbps.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2291			Network detection and response (NDR)		Existing Infrastructure Compatibility: Please provide details of the Bank's current network architecture (physical/virtual/cloud/hybrid) including switches, routers, and existing TAP/SPAN port availability for NDR sensor deployment.	Please refer addendum for revised clause
2292			Network detection and response (NDR)		Encrypted Traffic Analysis: Does the Bank require decryption capabilities for SSL/TLS encrypted traffic analysis, or is metadata-based/behavioral analysis on encrypted traffic sufficient without decryption?	Please refer addendum for revised clause
2293			Network detection and response (NDR)		Cloud Environment Coverage: Does the scope include monitoring of the Bank's cloud workloads (AWS/Azure/GCP) and hybrid environments, or is this limited to on-premise physical/virtual network infrastructure only?	Please refer addendum for revised clause
2294			Network detection and response (NDR)		Retention Requirements: What is the required data retention period for network traffic logs, packet captures (PCAP), and metadata for forensic and compliance purposes?	Please refer addendum for revised clause
2295			Network detection and response (NDR)		High Availability & DR: Kindly confirm the HA and DR requirements for the NDR solution, including RTO/RPO expectations, and whether the solution needs to be deployed in an Active-Active or Active-Passive configuration.	Please refer addendum for the revised deployment requirement
2296			Network detection and response (NDR)		Threat Intelligence Feeds: Does the Bank have existing Threat Intelligence subscriptions that need to be integrated with the NDR solution, or should the Bidder propose/include native/third-party threat intel feeds as part of the solution?	Bidder to proposed the solution as sort in the RFP
2297			Network detection and response (NDR)		Compliance & Data Sovereignty: In case of a SaaS-based solution, what are the specific regulatory/compliance requirements (RBI guidelines, data localization norms) that the Bidder must adhere to regarding data storage and processing location?	Please refer addendum for revised clause
2298			Network detection and response (NDR)		Sizing for On-Premise vs SaaS: For effort and cost estimation purposes, can the Bank confirm if a comparative proposal (SaaS vs. On-Premise) is acceptable, or is the evaluation strictly limited to one deployment model as per RFP scope?	Please refer addendum for revised clause
2299			Network detection and response (NDR)		Support & SLA Expectations: What are the expected SLA parameters (detection time, response time, uptime) for the NDR solution, and is 24x7 SOC-integrated support mandatory as part of the scope?	No Change, Please be guided by the RFP
2300			Network detection and response (NDR)		Implementation Timeline: Kindly confirm the expected project timeline for implementation, UAT, and Go-Live, along with any specific milestones the Bank has already defined, to help us plan resource allocation and effort sizing accurately.	Pleas be guided by the RFP Detailed project plan is to be submitted bidder and OEM for their respective solution and services.
2301		7.3.6	Decoy/HoneyPOT	A Decoy/HoneyPot solution should act as a decoy system that mimics sensitive financial systems, enticing attackers to engage with fake assets instead of real ones. This allows security teams to monitor attack patterns and behavior without compromising act ual banking infrastructure providing bank a unique opportunity to collect threat intelligence that can be used to reinforce security environment.	What is the total number of data centers, DR sites, cloud environments, and branch locations to be covered?	No Change, Please be guided by the RFP
2302			Decoy/HoneyPOT		What are the critical banking applications and systems to be replicated as decoys?	Details of solutions shall be shared with the selected bidder on a need-to-know basis.
2303			Decoy/HoneyPOT		Is there an existing deception platform deployed today? If yes, describe the current architecture and limitations.	Details will be shared with successful bidder
2304			Decoy/HoneyPOT		Should decoys mimic production naming conventions, IP schemes, certificates, and application banners?	The solution shall provide protection for web-facing, Internet-facing and Intranet-based applications associated with the Banking environment by enabling creation of custom decoys that emulate the actual application/server environment
2305			Decoy/HoneyPOT		What is the expected ratio of decoys to production assets?	Details of solutions shall be discussed with the selected bidder on a need-to-know basis. Bidder to proposed complying with the requirement stated in the RFP
2306			Decoy/HoneyPOT		How many network segments/VLANs require coverage?	Details shall be discussed with the successful bidder
2307		7.3.8 7.3.10	Vulnerability assessment (VA) & vulnerability lifecycle management Application security testing Tool	Generic	Please confirm the total number of assets (VMs, DBs, switch, routers, firewalls, WLC, APs, Load Balancers, and other infrastructure components) to be covered for Vulnerability assessment	No Change, Please be guided by the RFP
2308			Vulnerability assessment (VA) & vulnerability lifecycle management Application security testing Tool		Please share a bifurcation of number of assets for each physical location	Details shall be shared with the selected bidder on a need-to-know basis.
2309			Vulnerability assessment (VA) & vulnerability lifecycle management Application security testing Tool		For application security testing, please share the count of total number of web applications, mobile applications (android/iOS separately), APIs etc.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2310			Vulnerability assessment (VA) & vulnerability lifecycle management Application security testing Tool		VA Solution will be standalone deployments in DC & DR, separate for each. Are they also required to be in sync? Example: Vulnerabilities identified on assets in DC should reflect in the management console of DR, and vice-versa?	The VA solution shall be deployed as standalone deployments in DC and DR, separately. However, synchronization between the DC and DR VA deployments shall be achieved. Vulnerabilities identified on assets in the DC deployment shall be synchronized/reflected in the DR management console, and vulnerabilities identified on assets in the DR deployment shall likewise be synchronized/reflected in the DC management console, ensuring consistent and consolidated vulnerability visibility across both locations. The bidder shall ensure that all required licensing, architecture, integration and synchronization capabilities are included in the proposed solution to meet this requirement, without any additional cost to the Bank.
2311			Vulnerability assessment (VA) & vulnerability lifecycle management Application security testing Tool		Can we propose a SaaS solution for Vulnerability Management & Application Security Testing	No Change, Please be guided by the RFP
2312			Vulnerability assessment (VA) & vulnerability lifecycle management Application security testing Tool		Please mention all the physical locations, where on-premise deployments are required.	DC- Mumbai DR- Noida
2313			Vulnerability assessment (VA) & vulnerability lifecycle management Application security testing Tool		It is understood and assumed, PSB will procure, install, setup and manage the infrastructure components (VMs, servers, DB, storage, etc.) required for the functioning of the VA solution.	The bidder shall propose, size, supply and provide all infrastructure components required for the deployment and functioning of the VA solution, including but not limited to VMs/servers, database, storage and other requisite infrastructure components. The bidder shall ensure that the proposed infrastructure is adequate to meet all functional, performance, availability and deployment requirements specified in the RFP. The cost of all such required infrastructure shall be factored into the bidder's commercial proposal and shall not be treated as a separate Bank-provided dependency.
2314			Vulnerability assessment (VA) & vulnerability lifecycle management Application security testing Tool		Is it also expected to create policies, procedure, SOP documents?	No Change, Please be guided by the RFP
2315			Vulnerability assessment (VA) & vulnerability lifecycle management Application security testing Tool		It is understood and assumed that patch management, firmware	No Change, Please be guided by the RFP
2316			Vulnerability assessment (VA) & vulnerability lifecycle management Application security testing Tool		updates, software upgrades, security updates, bug fixes, configuration management, etc. are specific only to the deployed vulnerability management solution. However, patch management of the underlying infra i.e. VMs, OS, DB, etc. lies PSB.	The bidder shall be responsible for all updates, software upgrades, security updates, bug fixes, configuration management and maintenance required for the proposed VA and Application Security solution. However, where the bidder is responsible for providing the underlying infrastructure, the bidder shall also be responsible for its required maintenance and security updates.
2317			Vulnerability assessment (VA) & vulnerability lifecycle management Application security testing Tool		For application security testing, is manual testing also expected to be conducted, or is it limited to automated scanning via the tool?	The bidder shall ensure coverage of the applicable application security testing requirements specified in the RFP.
2318			Vulnerability assessment (VA) & vulnerability lifecycle management Application security testing Tool		Please confirm the scan frequency (weekly, monthly, quarterly)	Details shall be shared with the selected bidder on a need-to-know basis.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2319			Vulnerability assessment (VA) & vulnerability lifecycle management Application security testing Tool		Please confirm the scan methodology (authenticated or unauthenticated)	No Change, Please be guided by the RFP
2320			Vulnerability assessment (VA) & vulnerability lifecycle management Application security testing Tool		Tools based secure configuration review is also expected?	No Change, Please be guided by the RFP
2321		7.3.10	Application security testing Tool	The solution shall support scanning of container images from supported repositories/registries and integration with applicable CI/CD workflows.	Would it be acceptable if these capabilities are supported by the Cloud Security solution (CSPM/CNAPP), instead of a vulnerability management solution	No Change, Please be guided by the RFP
2322		Clause 7.1(l)(c–f), Clause 7.6.3(6,12), Clause 7.18(10–11)	Clause 7.1(l)(c–f), Clause 7.6.3(6,12), Clause 7.18(10–11)	Any unmentioned hardware, software, licenses, APIs, middleware or dependencies required for completeness must be supplied free of cost.	Please confirm that bidder liability is limited to items reasonably identifiable from the RFP, disclosed volumetrics and approved design, and that requirements arising from incomplete/incorrect Bank information will follow change control.	No Change, Please be guided by the RFP
2323		Clause 7.6(8), Clause 7.6.3(4)	Clause 7.6(8), Clause 7.6.3(4)	Unlimited customization, parser, connector, API, workflow, dashboard, report, tuning and remediation obligations throughout the contract at no extra cost.	Please define a baseline quantity/effort for integrations, parsers, playbooks, dashboards, reports and customization, with any excess processed through a priced CR mechanism.	No Change, Please be guided by the RFP
2324		Clauses 7.3.1.1(3,5–6)	Clauses 7.3.1.1(3,5–6)	Integration extends to all existing and future Bank systems and tools, creating unknown interface and third-party dependencies.	Please provide the complete current/future integration inventory, interface specifications, third-party responsibilities and annual growth forecast; confirm CR treatment for systems added after design freeze.	No Change, Please be guided by the RFP
2325		7.5(4)	7.5(4)			No Change, Please be guided by the RFP
2326		7.15(22)	7.15(22)			No Change, Please be guided by the RFP
2327		Clause 7.18	Clause 7.18	Bidder bears all sizing, growth, capacity and performance risk, including free augmentation and horizontal scaling.	Please confirm guaranteed baseline volumetrics and annual growth assumptions, and that growth beyond the stated scalable capacities/volumes will be procured at quoted unit rates rather than free augmentation.	No Change, Please be guided by the RFP
2328		Clauses 7.2.1–7.2.4	Clauses 7.2.1–7.2.4	Each node/environment must support full peak load, with N+N active-active at DC and DR, potentially multiplying infrastructure/license cost.	Please clarify whether "each node/environment full peak load" applies to every individual node, each site, or each HA pair, and provide the exact redundancy and licensing basis for every solution.	Clarification: Wherever HA is required, Each node—Primary and HA—should be capable of handling the full peak load on its own. If one node fails, the other node should be able to handle the complete load without any loss of required capacity. This requirement applies separately to each site.
2329		Clause 7.6.6(3)	Clause 7.6.6(3)	Development, Test, UAT and Pre-Production must be maintained throughout the contract; other clauses refer to production, training, development and test, creating environment ambiguity.	Please confirm the exact number, location, sizing and HA/DR requirements of non-production environments and whether SaaS licenses/resources for each are included in the commercial BoM.	Please refer addendum for revised clause
2330		Clause 7.18(9,19–21)	Clause 7.18(9,19–21)			No Change, Please be guided by the RFP
2331		Clauses 7.6.3(7), 7.13(45), 7.19.1(2,11–12),	Clauses 7.6.3(7), 7.13(45), 7.19.1(2,11–12),	Regulatory and Bank-policy changes are broadly included free of cost, but Clause 7.19.1 separately says new post-Go-Live functionality is on CR—an internal inconsistency.	Please reconcile the clauses and confirm that regulatory changes requiring new modules, licenses, material development or architecture changes will be handled through change request and commercial adjustment.	Regulatory or Bank-policy changes impacting existing functionality of the solution shall be provided at no additional cost during the contract period. However, where any such change requires entirely new functionality/module, additional licenses, or significant architecture/infrastructure changes that were not part of the existing solution at the time of Go-Live, the same shall be treated as a Change Request (CR) and shall be commercially evaluated based on the applicable rates in the Bill of Material. Accordingly, there is no inconsistency between the clauses; the distinction is between changes to existing functionality and new functionality/capabilities introduced after Go-Live.
2332		Clauses 7.12,7.12.3	Clauses 7.12,7.12.3	Bank can require additional onsite resources; some clauses say pro-rata payment, others require free augmentation to meet timelines/SLA/operations.	Please distinguish chargeable Bank-requested resource increases from bidder-funded SLA remediation and define objective triggers, approval and maximum free-augmentation period.	No Change, Please be guided by the RFP
2333		7.12.3	7.12.3	Dynamic use cases, reports, dashboards, SOP revisions and feature requests can be requested throughout the term, including critical feature delivery within one week.	Please state an annual baseline for new use cases/reports/ dashboards/features, acceptance criteria and prioritization; confirm additional requirements beyond baseline will use change control.	No Change, Please be guided by the RFP
2334		Clause 7.13(3,16), Clause 7.15(9–13), Annexure 25	Clause 7.13(3,16), Clause 7.15(9–13), Annexure 25	Dynamic use cases, reports, dashboards, SOP revisions and feature requests can be requested throughout the term, including critical feature delivery within one week.	Please state an annual baseline for new use cases/reports/dashboards/features, acceptance criteria and prioritization; confirm additional requirements beyond baseline will use change control.	No Change, Please be guided by the RFP
2335		Clause 7.15(9–13),Clause 7.13(18)	Clause 7.15(9–13),Clause 7.13(18)	At least 15 unique use cases per business application within six months of Go-Live could mean about 3,000 use cases for 200 stated applications, subject to application readiness.	Please confirm the number of applications in scope for this obligation, what qualifies as a unique use case, target acceptance criteria, app-owner dependencies and whether the count is solution-wide or per application.	Details shall be discussed with succesfull bidder
2336		Clause 7.19.2(1–5)	Clause 7.19.2(1–5)	Existing estate takeover from 01/05/2027 on "as-is, where-is" while full SLAs apply; asset health, licenses, documentation and incumbent cooperation are unknown.	Please share the existing estate inventory, license/support status, backlog, known defects, architecture and SLA history; provide a discovery/stabilization period during which inherited defects are excluded from SLA/penalty.	Details shall be shared with successful bidder

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2337		Clause 7.19.2(4)	Clause 7.19.2(4)	Existing SIEM must run for 12 months after Go-Live, creating dual-run cost, staffing, license and integration obligations.	Please clarify who bears incumbent license/OEM support/infrastructure costs, whether existing and new SIEM SLAs both apply, and the exact exit/ decommissioning criteria.	The existing SIEM shall continue to be operated for a period of 12 months after Go-Live of the proposed SIEM, primarily to support regulatory, audit and transition requirements. The Bidder shall be required to provide necessary support for the continued running of the existing SIEM during this period on best effort basis.
2338		Clause 7.2.4.3(1)(d)	Clause 7.2.4.3(1)(d)	All cloud ingress/egress, inter-zone transfer, API, backup, retrieval, migration and exit costs are included, but actual data movement is uncertain.	Please provide expected monthly ingress/egress, restoration and archival retrieval volumes, regions/zones and migration/exit scenarios; allow rate adjustment for usage above the disclosed baseline.	Bidders shall size the solution using the RFP volumetrics and growth requirement.
2339		Clause 11,Clause 14.2	Clause 11,Clause 14.2	Bank may increase/decrease quantities by 25% at same unit prices and descope components before award; dependencies and stranded costs may remain with bidder.	Please confirm minimum committed quantities/value, treatment of OEM minimum commitments and non-cancellable cloud/license orders, and equitable price adjustment where descope changes architecture or unit economics.	No Change, Please be guided by the RFP
2340		Clause 7.13(46), Clause 7.18.5	Clause 7.13(46), Clause 7.18.5	New OEM features and capabilities activated only by license must be provided free; committed functionality must remain despite OEM SKU/licensing changes.	Please limit free entitlement to features included in the contracted SKU/support plan and clarify treatment of separately priced modules, acquisitions and materially new products.	No Change, Please be guided by the RFP
2341		Clause 7.13(8–9),	Clause 7.13(8–9),	Quarterly or ad-hoc DR drills, regulator drills and full manpower deployment can create unplanned effort and business-hours impact.	Please define the annual number, duration, notice period and success criteria for planned/unplanned drills and confirm treatment of exercises above the agreed baseline.	No Change, Please be guided by the RFP
2342		Clause 13.1(16), Services SLA	Clause 13.1(16), Services SLA	SLA scope contains possible drafting errors, such as reference to Core/Perimeter Firewall and anti-rogue/antimalware, although these are not the central scope.	Please confirm that firewall/anti-rogue/antimalware penalties apply only to components explicitly awarded under this RFP and remove references to out-of-scope solutions.	Please refer addendum for revised clause.
2343		Clauses 14.8, 14.13, 14.20–14.21,	Clauses 14.8, 14.13, 14.20–14.21,	Liability carve-outs may be uncapped and indemnities are broad, including regulatory fines, confidentiality, IP and DPDP exposures.	Please apply the overall liability cap or a negotiated super-cap to all claims except fraud/willful misconduct, and clarify that indemnity applies only to direct losses caused by bidder breach and finally imposed fines.	Pleas be guided by the RFP
2344		Clause 14.1, Clause 7.12.5(11)	Clause 14.1, Clause 7.12.5(11)	Subcontracting is prohibited, which may conflict with cloud providers, OEM affiliates, specialized takedown providers and other embedded delivery partners.	Please confirm that approved OEMs, OEM affiliates and specialist service delivery partners named in the bid are permitted and do not constitute prohibited subcontracting.	Pleas be guided by the RFP
2345		Clause 7.6.8(6), Clause 7.7(11)	Clause 7.6.8(6), Clause 7.7(11)	Bank data cannot be accessed outside India, which may conflict with global OEM support and follow-the-sun operations.	Please clarify whether metadata-only remote support is permitted, define approval process for offshore OEM SMEs, and confirm required India-based support model and data-access controls.	Pleas be guided by the RFP
2346		Clause 10.4(8),	Clause 10.4(8),	Bank may add “any other relevant criteria” for commercial evaluation, creating post-bid uncertainty.	Please delete or restrict this right to objective criteria disclosed through a pre-bid corrigendum before bid submission.	Please refer addendum for the revised clauses in the overall RFP
2347		Clause 13.2, Clause 14.19	Clause 13.2, Clause 14.19	Implementation LD is inconsistently stated at 1% per week of Product Cost and 0.5% per week of Contract Price, creating overlapping exposure.	Please confirm which LD rate/base applies to each delay category and that the two provisions will not be applied cumulatively for the same delay.	No Change, Please be guided by the RFP
2348		Clause 7.18(3), Clause 7.1(l)(a)	Clause 7.18(3), Clause 7.1(l)(a)	Hardware must be “not older than 2025,” latest/stable, supported through contract plus extension; refresh obligations may arise mid-term at bidder cost.	Please clarify the meaning of “not older than 2025,” lifecycle cut-off at bid/delivery, and whether capacity-neutral technology refresh due solely to OEM lifecycle is included or separately compensated.	Please refer addendum for revised clause.
2349		7.4.8	Threat hunting Services	The Bidder shall provide offsite, tool-based, proactive and intelligence-driven threat hunting services to identify advanced threats, malicious activities, unknown attack techniques, and indicators of compromise that may evade the Bank's existing security controls. The service shall include, but not be limited to: a. Proactive threat hunting across endpoint, network, cloud, identity, application, and AI environments, wherever applicable. b. IOC, IOA, and TTP-based investigation. c. Behavioral analytics and anomaly detection. d. Threat intelligence-driven threat hunting. e. Investigation of suspected advanced persistent threats and emerging attack techniques. f. Detection engineering and security use-case tuning. g. Correlation rule optimization. h. Validation and assessment of SOC detection capabilities. maintenance & management of NextGen SOC & related services I. Identification of gaps in existing detection and monitoring mechanisms. j. Recommendations for remediation and improvement of security controls. k. Periodic threat hunting reports, findings, risk assessment, and executive dashboards. l. Tracking of identified findings and recommended remediation actions. m. The threat hunting service shall be delivered remotely/offsite using secure and mutually agreed mechanisms for	Environment Coverage & Scale: Kindly provide the total count of endpoints, servers, network devices, cloud workloads (IaaS/PaaS/SaaS), identity systems, and applications that will be in scope for threat hunting, to enable accurate effort estimation.	No Change, Please be guided by the RFP, sizing is to be done based on the provided information
2350			Threat hunting Services		Log Source Access: What are the specific log sources, telemetry, and security tools (SIEM, EDR, NDR, CASB, IAM, etc.) that will be made available to the Bidder for offsite threat hunting, and what is the expected data retention/lookback period accessible for investigation?	Details shall be shared with successful bidder
2351			Threat hunting Services		Access Mechanism: Please elaborate on the "secure and mutually agreed mechanism" for offsite access – will this be via VPN, Jump Server, VDI, or a dedicated secure remote access tool provided by the Bank?	Clarification: The specific access mode (VPN, Jump Server, VDI, or a Bank-provisioned secure remote-access tool) is intentionally not prescribed in the RFP and shall be finalized mutually with the successful Bidder, based on the Bank's prevailing information-security policy and the nature of the tool/data being accessed. This ensures the mechanism aligns with the Bank's security posture at the time of implementation.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2352			Threat hunting Services		Frequency of Threat Hunting: What is the expected frequency of proactive threat hunting exercises (e.g., weekly, bi-weekly, monthly) versus continuous/on-demand hunting based on emerging threat intelligence?	The bidder shall conduct proactive threat hunting at least once every month as a scheduled activity. In addition, the bidder shall undertake event-driven/on-demand threat hunting whenever warranted by emerging threat intelligence, significant vulnerabilities, suspected compromise, security incidents, or newly identified Indicators of Compromise (IOCs) / Tactics, Techniques and Procedures (TTPs). The monthly threat-hunting activity shall be documented and reported to the Bank. Additional threat hunting arising from security incidents or credible emerging threats shall be included within the scope of the managed security service and shall not be treated as a separate charge.
2353			Threat hunting Services		AI Environment Scope: Could the Bank elaborate on what constitutes the "AI environment" mentioned in the scope (e.g., AI/ML models, MLOps pipeline, AI-based applications) so that we can assess the specific skillsets and tools required?	No Change, Please be guided by the RFP Clarification: The scope covers threat hunting for security risks arising from the Bank's AI/ML-enabled systems and workloads as and when deployed by the Bank, including but not limited to AI/ML models, associated pipelines, and AI-based applications, to the extent such environments exist within the Bank's IT landscape
2354			Threat hunting Services		Detection Engineering Scope: For "detection engineering and correlation rule optimization" – does the Bank expect the Bidder to have write-access to create/modify use-cases and correlation rules directly in the SIEM/SOC tools, or only provide recommendations for the Bank's SOC team to implement?	No Change, Please be guided by the RFP
2355			Threat hunting Services		Number of Use-Cases: What is the current number of active correlation rules/use-cases deployed in the SOC that would require periodic tuning, validation, and optimization as part of this engagement?	Details shall be discussed with the successful bidder
2356			Threat hunting Services		Reporting Cadence: What is the expected frequency and format for periodic threat hunting reports, executive dashboards, and risk assessments (e.g., weekly operational reports, monthly executive summary, quarterly risk review)?	The bidder shall conduct proactive threat hunting at least once every month as a scheduled activity. In addition, the bidder shall undertake event-driven/on-demand threat hunting whenever warranted by emerging threat intelligence, significant vulnerabilities, suspected compromise, security incidents, or newly identified Indicators of Compromise (IOCs) / Tactics, Techniques and Procedures (TTPs). The monthly threat-hunting activity shall be documented and reported to the Bank. Additional threat hunting arising from security incidents or credible emerging threats shall be included within the scope of the managed security service and shall not be treated as a separate charge.
2357			Threat hunting Services		SLA for Findings & Remediation Tracking: Are there specific SLAs expected for closure/tracking of identified findings and remediation actions, and will the Bidder be required to use the Bank's existing ITSM/GRC tool for tracking, or propose its own?	No Change, Please be guided by the RFP
2358			Threat hunting Services		Team Composition & Certifications: Does the Bank have specific requirements regarding the certifications (e.g., GCTI, GNFA, OSCP, CEH) and minimum experience level of threat hunters to be deployed for this engagement?	No Change, Please be guided by the RFP
2359			Threat hunting Services		APT/Emerging Threat Scope: For "investigation of suspected APTs and emerging attack techniques," is this limited to reactive investigation upon detection, or does the Bank expect continuous proactive research on threat actor groups relevant to the BFSI sector?	No Change, Please be guided by the RFP
2360			Threat hunting Services		Validation of SOC Capabilities: Could the Bank clarify the expected scope and periodicity for "validation and assessment of SOC detection capabilities" – is this a one-time baseline assessment, or an ongoing/periodic exercise (e.g., quarterly Purple Team exercises)?	No Change, Please be guided by the RFP, refer section 7.6.5 Deployment and Go-Live
2361		ITDR	1.7	Detect and respond to active threats with high fidelity (low false positives and false negatives).	Pre-Bid Query / Clarification: The Bank has separately specified a comprehensive deception platform for detection of active attacker activity, reconnaissance and lateral movement. We understand that the intent of this clause within ITDR is therefore to complement those controls with focused monitoring of the Bank's most critical identities. Considering that enhanced user-activity monitoring is most relevant for high-risk personnel such as executives, privileged users and other critical users, we request the Bank to kindly clarify whether this requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should provide high-fidelity detection and response for risky or anomalous user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, to identify activities associated with careless, malicious or compromised users.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2362		ITDR	1.8	Provide contextual information—who, what, when and how—to inform all stages of the attack chain.	Pre-Bid Query / Clarification: The Bank has already sought attack-lifecycle visibility under the separate deception requirements. For ITDR, we understand that additional value would be derived from detailed user-centric context for the Bank's most critical identities, enabling investigation of risky activity performed by such users. We request the Bank to kindly clarify whether this requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should provide contextual information—who, what, when, where and how—around risky user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, to support investigation and response.	No Change, Please be guided by the RFP
2363		ITDR	1.9	Provide deep insights into both the potential and used privilege escalation and lateral movement steps in an attack.	Pre-Bid Query / Clarification: Privilege escalation and lateral-movement visibility is already substantially addressed under the separately specified deception solution, including attacker lifecycle visibility, MITRE ATT&CK mapping, deceptive attack paths and detection of lateral movement. To avoid duplication while retaining complementary investigation capability for high-risk identities, we request the Bank to kindly clarify whether this requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should provide deep insights into activities performed by up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, covering application usage, file and data movement, endpoint activity and other risky behaviours to support investigation of compromised, malicious or negligent user activity.	No Change, Please be guided by the RFP
2364		ITDR	2.9	Detect all types of attack vectors including pre-attack reconnaissance, zero-day attacks, privilege escalation prevention, lateral movement and data theft.	Pre-Bid Query / Clarification: Pre-attack reconnaissance, lateral movement, malware/attack behaviour and attacker lifecycle visibility are already covered under the Bank's separate deception specifications. We understand that the complementary requirement under ITDR should focus on identity/user risk and potential data-loss activity for the Bank's most critical users rather than duplicate the deception control. We request the Bank to kindly clarify whether this requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should detect risky user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, including suspicious application usage, unauthorized access or movement of sensitive information, removable-media activity, web-based transfer, cloud synchronization and other potential data-exfiltration activities.	The Clause is applicable only to idendity related threat vector only. The volumetrics is provided in the RFP and should be complied
2365		ITDR	2.10	Detect multiple attacks simultaneously.	Pre-Bid Query / Clarification: We understand the intent is to ensure that the solution is not restricted to investigation of a single event at a time. Since active attacker detection is separately covered by the deception solution, we request that this clause be clarified in terms of concurrent monitoring and investigation of risky activities across the Bank's designated critical-user population: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should be capable of detecting and investigating multiple risky user and data activities simultaneously across up to 100 critical/high-risk users and their monitored endpoints.	No Change, Please be guided by the RFP
2366		ITDR	3.2	Provide unified presentation of both source- and target-based telemetry data in a timeline view.	Pre-Bid Query / Clarification: The Bank has separately specified end-to-end attacker visibility and behavioural analysis under the deception solution. For ITDR investigations involving critical identities, a chronological user-activity view would provide complementary evidence of actions performed by the user. We request the Bank to kindly clarify whether the requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should provide a unified chronological timeline of user- and endpoint-based activity telemetry for up to 100 critical/high-risk users identified by the Bank to support investigation of risky or suspicious user activity.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2367		ITDR	3.3	Correlate identity-related telemetry from relevant source and target systems to identify and investigate identity compromise, privilege escalation, credential abuse and lateral movement.	Pre-Bid Query / Clarification: Privilege escalation and lateral-movement detection are already addressed through the separately specified deception controls. To provide complementary investigation capability for the Bank's highest-risk identities, we request the Bank to clarify whether this clause may focus on correlation of user, endpoint, application and data activity for the designated critical-user population: Suggested Clarified Wording / Requested Action: The solution shall support correlation of user, endpoint, application and data-activity telemetry for up to 100 critical/high-risk users identified by the Bank to identify and investigate suspicious user behaviour, sensitive-data movement, policy violations and potential data-exfiltration activities.	No Change, Please be guided by the RFP
2368		ITDR	3.4	Integrate with compatible endpoint/extended detection solution to capture screen recordings or screenshots during active attacker sessions as advanced forensic evidence.	Pre-Bid Query / Clarification: The Bank has separately specified attacker-session and forensic visibility through the deception platform. Within ITDR, we understand that visual evidence is intended to strengthen investigation of high-risk user activity. We request the Bank to kindly clarify whether the requirement may be read in an outcome-based manner for the designated critical-user population: Suggested Clarified Wording / Requested Action: The Identity Threat Detection Solution should support screenshots, screen capture or equivalent visual evidence of relevant activity for up to 100 critical/high-risk users during suspicious or high-risk user sessions, as part of forensic investigation and evidence collection.	Please refer addendum for revised clause
2369		ITDR	3.5	Integrate with compatible network detection solution to support collection of PCAP data for network-level incident visibility.	Pre-Bid Query / Clarification: The requirement for PCAP is network-centric and does not directly relate to identity posture or focused user-activity monitoring. Further, the Bank's separate deception specifications already require high-interaction decoys, recording of attacker activities, traffic/behaviour visibility, forensic investigation and integration with network/security technologies. To avoid duplication of network-level forensic controls across two solution categories, we request the Bank to kindly delete this clause from the ITDR section. Suggested Clarified Wording / Requested Action: Requested action: Delete Clause 3.5 from the ITDR requirements, as equivalent/complementary network and attacker forensic visibility is already sought under the separate Deception requirements.	Please refer addendum for revised clause
2370		ITDR	3.6	Push incident data into SIEM/XDR or SOAR technologies via integrations for improved incident management.	Pre-Bid Query / Clarification: We understand that the objective is to ensure relevant ITDR alerts and investigation context are available to the Bank's SOC ecosystem. For the enhanced monitoring of designated critical users, we request the Bank to kindly clarify whether alerts and activity information may be shared through supported integrations or APIs as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should make alerts and relevant incident/activity data for the monitored critical-user population available to SIEM/XDR, SOAR or other supported security platforms through integrations or APIs for improved incident management.	The proposed solution hould be integrated with SIEM/XDR or SOAR technologies for sharing the incident data via supported integrattion or APIs
2371		ITDR	3.7	As part of forensic data collection, include detailed attack path information including protocols leveraged during the attack.	Pre-Bid Query / Clarification: Detailed attack-path and attacker-behaviour visibility is already sought under the separate deception specifications, including deceptive attack paths, MITRE ATT&CK mapping and forensic investigation. To avoid overlap while retaining complementary evidence for investigations involving the Bank's critical identities, we request the Bank to kindly clarify whether the requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should, as part of forensic data collection for up to 100 critical/high-risk users, include detailed user-activity information such as applications used, files accessed, data movement, destination channels and other relevant endpoint activity associated with the incident.	Please refer addendum for revised clause
2372		ITDR	3.8	Collect user and computer information from Active Directory as part of forensic data gathering to enhance context and assess risk exposure.	Pre-Bid Query / Clarification: We understand that directory information is required to enrich investigations with user and computer context. We request the Bank to clarify that enterprise identity context may be maintained for the overall identity population, while detailed endpoint/user-activity telemetry may be applied to the Bank's designated critical-user population: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should use relevant user and computer identity information to enhance forensic context and risk assessment, and should correlate such context with detailed endpoint/user-activity telemetry for up to 100 critical/high-risk users identified by the Bank.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2373		ITDR	3.9	Detect an adversary's attempt to move laterally toward key assets using as many Windows, Mac or Linux hosts as possible without requiring a persistent agent.	Pre-Bid Query / Clarification: The Bank's separate deception specifications expressly require detection of lateral movement, reconnaissance, credential theft and malicious activity using agentless and/or agent-based deception techniques across the enterprise. The present clause therefore duplicates a capability already being procured under the Deception section. To avoid overlapping scope and duplicate controls, we request the Bank to kindly delete this clause from the ITDR section. Suggested Clarified Wording / Requested Action: Requested action: Delete Clause 3.9 from the ITDR requirements, since lateral-movement detection using deception techniques is already explicitly covered under the separate Deception specifications.	Please refer addendum for revised clause
2374		ITDR	3.10	Collect AD user/computer information for forensic context and detect at the earliest point post initial compromise as the attacker first attempts lateral movement and privilege escalation.	Pre-Bid Query / Clarification: Early detection of lateral movement and privilege-escalation activity is substantially covered under the Bank's separate deception requirements. To retain a complementary identity/user-risk objective without duplicating the deception scope, we request the Bank to kindly clarify whether this clause may focus on early detection of risky activity among the designated critical-user population: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should use relevant identity context and detect risky user behaviour at the earliest possible point for up to 100 critical/high-risk users, based on monitored endpoint activities and configured detection policies, enabling investigation and response before such activity results in significant data loss or business impact.	Please refer addendum for revised clause
2375		ITDR	3.11	Collect AD user/computer data during forensic gathering while ensuring all deception techniques remain hidden from legitimate users.	Pre-Bid Query / Clarification: The requirement to ensure deception techniques remain hidden from legitimate users is inherently a deception-platform capability. The Bank has already included comprehensive deception requirements covering lures, breadcrumbs, fake credentials, deceptive assets, attacker engagement and techniques designed to remain undetected by attackers. We therefore request the Bank to kindly delete this clause from the ITDR section to avoid duplication. Suggested Clarified Wording / Requested Action: Requested action: Delete Clause 3.11 from the ITDR requirements, as deception techniques and their concealment are already covered under the separate Deception specifications.	Please refer addendum for revised clause
2376		Anti Phishing	17.1	Solution should detect at the earliest point in the attack, post initial compromise as the attacker is first attempting to move laterally and escalate privilege.	Pre-Bid Query / Clarification: Since this section is focused on Anti-Phishing, we understand that the objective is to identify suspicious activity following a successful phishing or account-compromise event. Network-level lateral movement and deception capabilities may be addressed by other security controls. We request the Bank to clarify whether this clause may instead focus on early post-compromise user activity visibility for the Bank's most critical users. Suggested Clarified Wording / Requested Action: The solution should support early identification and investigation of suspicious user activities associated with potential account compromise following phishing or other email-originated attacks, with enhanced user activity monitoring for up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles.	Please refer to the relevant Addendum for updated specfications
2377		Anti Phishing	17.4	Solution must provide robust supply chain and AI/ML-driven contact chain analysis capabilities to identify and defend against socially engineered, impersonated, or BEC attacks.	Pre-Bid Query / Clarification: As compromise of trusted suppliers and partners is an important source of BEC and phishing risk, we request the Bank to clarify whether the existing supply-chain requirement should explicitly include behavioural analysis of supplier/partner communication patterns to identify attacks originating from compromised trusted accounts. Suggested Clarified Wording / Requested Action: Solution must provide robust supply-chain and AI/ML-driven contact-chain and behavioural analysis capabilities to identify and defend against socially engineered, impersonated or BEC attacks, including threats originating from compromised or impersonated supplier/partner accounts.	Please refer to the relevant Addendum for updated specfications
2378		Anti Phishing	18	Solution must proactively analyze suspicious URLs using dynamic/behavioral analysis to prevent the spread of malware and other threats.	Pre-Bid Query / Clarification: The RFP separately addresses URL analysis and post-delivery remediation. We request clarification whether these requirements are intended to provide continuous protection throughout the email threat lifecycle, including pre-delivery analysis, click-time URL protection and post-delivery detection/remediation. Suggested Clarified Wording / Requested Action: Solution must provide continuous protection across the email threat lifecycle, including pre-delivery threat detection, real-time/click-time inspection of suspicious URLs, and post-delivery detection and automated remediation of threats that are subsequently determined to be malicious.	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2379		Anti Phishing	19.7	Solution must be able to offer a comprehensive portal that allows users to access information and metadata on events/incidents, facilitating network threat forensics for thorough investigation and analysis of potential security breaches or incidents.	Pre-Bid Query / Clarification: To strengthen investigation of phishing-led incidents involving executives and other critical users, we request clarification whether the existing forensic portal requirement may also include contextual user and endpoint activity for a limited population of Bank-identified critical/high-risk users. Suggested Clarified Wording / Requested Action: Solution must offer a comprehensive investigation portal providing information and metadata on events/incidents for forensic analysis. For up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, the portal should additionally provide contextual user and endpoint activity, including relevant application, file and user-action details, to support investigation of potential phishing-led compromise.	Please refer to the relevant Addendum for updated specfications
2380		Anti Phishing	19.9	Solution must empower security operations and incident responders to automate the identification, remediation, and sharing of phishing threats, streamlining the process of detecting, addressing, and disseminating information about potential phishing attacks for improved response and mitigation.	Pre-Bid Query / Clarification: To improve SOC investigation efficiency, we request clarification whether the existing phishing identification and remediation requirement should include centralized attack context showing why a message was identified as malicious, the users targeted, associated threat indicators and remediation status. Suggested Clarified Wording / Requested Action: Solution must empower security operations and incident responders to automate identification, investigation, remediation and sharing of phishing threats, and should provide centralized contextual visibility into the users targeted, associated threat indicators, detection rationale, attack characteristics and remediation actions.	Please refer to the relevant Addendum for updated specfications
2381		Anti Phishing	19.1	Solution must provide incident responders with real-time analytics and visibility into email-based attacks targeting the organization.	Pre-Bid Query / Clarification: Email-based attacks against executives and privileged users may require additional context after delivery to determine whether a targeted user has subsequently performed suspicious activity. We request the Bank to clarify whether real-time investigation visibility may include relevant user activity context for up to 100 Bank-identified critical/high-risk users. Suggested Clarified Wording / Requested Action: Solution must provide incident responders with real-time analytics and visibility into email-based attacks targeting the organization. For up to 100 Bank-identified critical/high-risk users, the solution should additionally provide contextual visibility into suspicious user activities associated with potential phishing or account compromise, including relevant user, endpoint, application and file activity.	Please refer to the relevant Addendum for updated specfications
2382		Anti Phishing	19.23	Solution must have simplicity of evaluation and additional visibility into internal traffic and other communication channels can reduce risk, and baseline user activity to detect suspicious behavior.	Pre-Bid Query / Clarification: The existing clause already seeks baselining of user activity to detect suspicious behaviour. We request the Bank to clarify the intended depth and scope of this capability and whether enhanced monitoring may be applied to a focused population of up to 100 Bank-identified critical/high-risk users, where deeper visibility provides the greatest security value. Suggested Clarified Wording / Requested Action: Solution must provide additional visibility into relevant internal activity and communication channels to reduce risk and baseline user activity to detect suspicious behaviour. Enhanced user and data activity monitoring should be provided for up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, with configurable detection policies for suspicious, anomalous or policy-violating activities.	Please refer to the relevant Addendum for updated specfications
2383		Anti Phishing	19.7	Solution must provide protection against harassment mail and mitigate the risks associated with emails from unknown senders specifically for executives or VIPs, safeguarding them from potential threats and ensuring their email communication remains secure.	Pre-Bid Query / Clarification: Since this clause already provides enhanced protection for executives/VIPs, we request the Bank to clarify whether such enhanced protection should extend beyond receipt of suspicious email to investigation of risky user and data activities that may occur following phishing or account compromise, for a limited set of the Bank's most critical users. Suggested Clarified Wording / Requested Action: Solution must provide protection against harassment mail and mitigate risks associated with emails from unknown senders specifically for executives or VIPs. For up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, the solution should additionally provide enhanced visibility into risky user and data activities following suspected phishing or account compromise, including relevant file movement, web/upload activity, removable-media activity and other supported data-transfer channels.	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2384		Cloud	1	OEM shall ensure compliance of the complete proposed solution & platform with RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and all applicable regulations throughout the contract period.	Pre-Bid Query / Clarification: We request the Bank to clarify that the OEM is required to maintain applicable security, privacy and regulatory controls relevant to the services provided and furnish available compliance/assurance documentation, while the overall regulatory compliance obligation of the Bank remains subject to the Bank's deployment, configuration and usage of the service. Suggested Clarified Wording / Requested Action: OEM shall maintain security, privacy and compliance controls applicable to the proposed hosted service and shall provide available independent assurance reports, certifications and relevant compliance documentation to support the Bank's obligations under applicable RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and other applicable regulatory requirements.	Please refer addendum for revised clause
2385		Cloud	2	The Service uptime agreement for the proposed solution on cloud should have monthly uptime commitments and have transparent monthly credit calculations in case of uptime not being met for any services.	Pre-Bid Query / Clarification: We understand that published/contracted OEM hosted-service SLA commitments and corresponding service-credit methodology shall meet this requirement. Kindly confirm. Suggested Clarified Wording / Requested Action: Retain clause, with clarification that the applicable OEM hosted-service SLA and service-credit schedule will govern the commitment.	No Change, Please be guided by the RFP
2386		Cloud	3	Solution provider should provide the design and process for data deletion in the scope of an independent audit and that the operational effectiveness of these controls is tested. The report for the same should be submitted to bank as and when asked by bank.	Pre-Bid Query / Clarification: For a globally operated hosted security service, control effectiveness is generally evidenced through independent assurance reports such as SOC 2 Type II and documented data-retention/deletion controls. We request the Bank to permit such independent assurance documentation instead of requiring a separate bespoke data-deletion audit report. Suggested Clarified Wording / Requested Action: Solution provider shall maintain documented secure data-retention and deletion controls. Compliance may be demonstrated through applicable independent third-party assurance reports/certifications (such as SOC 2 Type II or equivalent) and documented data-retention/deletion policies made available subject to OEM confidentiality requirements.	Please refer addendum for the revised clause
2387		Cloud	4	Independent audit for testing effectiveness of secure data removal, such that data is rendered permanently inaccessible. (Including any backup or distributed online media).	Pre-Bid Query / Clarification: We request the Bank to accept independently audited secure deletion and media-management controls, together with documented retention/deletion periods, rather than requiring a customer-specific audit of all backup and distributed media. Suggested Clarified Wording / Requested Action: The OEM shall maintain secure data deletion, media handling and backup-retention controls designed to render customer data inaccessible in accordance with documented retention schedules. Effectiveness may be evidenced through independent assurance reports such as SOC 2 Type II/ISO 27001 or equivalent and relevant OEM security/privacy documentation.	Please refer addendum for the revised clause
2388		Cloud	5	Bank shall have an option to implement 'Bring Your Own Key' as and when required.	Pre-Bid Query / Clarification: The proposed service protects data at rest and in transit using strong encryption; however, customer-managed infrastructure encryption keys are not a standard capability of the hosted anti phishing service. We request deletion of the BYOK requirement, or acceptance of OEM-managed enterprise-grade encryption and key-management controls. Suggested Clarified Wording / Requested Action: Requested Action: Delete the BYOK requirement. Alternatively: 'Data processed/stored by the hosted service shall be protected using industry-standard encryption in transit and at rest, with secure OEM-managed key-management controls subject to independent security assurance.'	Please refer addendum for the revised clause
2389		Cloud	6	Web Application Firewall shall be implemented on the cloud for Web based applications. WAF application signature should be updated and reviewed regularly. The Report shall be submitted to bank on a periodic interval.	Pre-Bid Query / Clarification: Since the proposed platform is an OEM-managed hosted security service, underlying WAF technology, signatures and configurations form part of the OEM's internal security architecture and may not be exposed as customer-specific reports. We request the Bank to accept periodic VAPT/penetration-test assurance or equivalent independent security assessment evidence covering the hosted application instead of WAF signature reports. Suggested Clarified Wording / Requested Action: The hosted web application/platform shall be protected through appropriate application-security controls. The OEM shall conduct periodic vulnerability assessment and penetration testing/security assessments and, subject to confidentiality restrictions, provide an executive summary/attestation or applicable independent assurance evidence to the Bank on request. Customer-specific WAF signature reports shall not be mandatory.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2390		Cloud	7	The systems in cloud infrastructure should be periodically updated with the latest anti-malware signatures, the bidder shall submit the periodic report on the same with bank.	Pre-Bid Query / Clarification: For an OEM-managed hosted security service, infrastructure anti-malware/endpoint controls are centrally managed and independently audited. We request the Bank to accept OEM security assurance and vulnerability/malware-control attestations rather than periodic host-level signature reports. Suggested Clarified Wording / Requested Action: The OEM shall maintain appropriate malware protection, vulnerability management, patching and security monitoring controls for the hosted infrastructure. Compliance may be evidenced through independent assurance reports/certifications and applicable security-control attestations instead of customer-specific anti-malware signature update reports.	Please refer addendum for revised clause
2391		Cloud	8	Data Loss Governance and risk management framework shall be defined by bidder for workload on the cloud and same shall be shared with bank on periodic basis. Data loss prevention controls should be implemented to secure the data in the cloud environment from unauthorized or inadvertent exfiltration.	Pre-Bid Query / Clarification: We request clarification that the requirement is intended to ensure protection against unauthorized/inadvertent data exfiltration through the proposed service and appropriate security controls for hosted customer data, rather than requiring disclosure of the OEM's internal cloud governance framework. Suggested Clarified Wording / Requested Action: The proposed solution shall provide configurable controls to identify and prevent unauthorized or inadvertent transmission/exfiltration of sensitive information through any channels. The OEM shall maintain appropriate access control, encryption and data-protection controls for customer data processed within the hosted service and provide applicable assurance documentation on request.	Please refer addendum for revised clause
2392		Cloud	9	Log generation, storage and review process should be certified by CERT IN empaneled auditor, report for the same shall be submitted by bidder as and when required by bank.	Pre-Bid Query / Clarification: For global SaaS/POD services, security logging and monitoring controls are typically independently audited under recognized assurance frameworks. We request the Bank to accept SOC 2 Type II/ISO 27001 or equivalent independent assurance in lieu of a mandatory CERT-In-empanelled audit of the OEM's internal log-generation/storage/review process. Suggested Clarified Wording / Requested Action: The OEM shall maintain documented security logging, monitoring, retention and review controls. Effectiveness shall be evidenced through applicable independent third-party assurance reports/certifications such as SOC 2 Type II, ISO 27001 or equivalent. CERT-In-empanelled audit may be required only for bidder-managed components deployed specifically within the Bank environment, where applicable.	Please refer addendum for the revised clause
2393		Cloud	10	IT Act 2000 & its amendments, and other Acts/Regulatory guidelines.	Pre-Bid Query / Clarification: Kindly clarify that the OEM must comply with legal/regulatory requirements applicable to it as the provider of the proposed hosted service and provide reasonable documentation to support the Bank's compliance obligations. Suggested Clarified Wording / Requested Action: OEM shall comply with applicable legal and regulatory obligations relevant to its provision of the proposed service and shall provide available security/privacy/compliance documentation reasonably required to support the Bank's applicable obligations.	Please refer addendum for the revised clause
2394		Cloud	11	CERT IN Empaneled auditor report's is required for the following:	Pre-Bid Query / Clarification: We request the Bank to permit internationally recognized independent assurance reports/certifications for OEM-managed hosted services. CERT-In empanelled audit reports may remain applicable to India-specific bidder-managed/on-premises components where such audit is feasible and required. Suggested Clarified Wording / Requested Action: For OEM-managed hosted/SaaS services, independent assurance reports/certifications such as SOC 2 Type II, ISO 27001 or equivalent shall be accepted. CERT-In empanelled audit reports shall be applicable only to components/services for which such India-specific audit is contractually and technically feasible.	Please refer addendum for the revised clause
2395		Cloud	12	The application and DB is/will be hosted separately on a dedicated infrastructure (physical/logical) for PSB. Evidence of dedicated infrastructure (physical/logical) for PSB should be submitted.	Pre-Bid Query / Clarification: The proposed platform is an OEM-managed hosted security service designed with logical access controls and customer data isolation. Requiring dedicated physical application/database infrastructure would restrict standard SaaS/POD architectures without necessarily improving the security outcome. We request acceptance of secure logical tenant/customer isolation supported by independent assurance evidence. Suggested Clarified Wording / Requested Action: The proposed hosted service shall provide secure logical segregation/isolation of Bank data and administrative access from other customers through appropriate access-control and tenant-isolation mechanisms. Dedicated physical application/database infrastructure shall not be mandatory where equivalent logical isolation is implemented and independently assured.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2396		Cloud	13	Feasibility to audit/review IT controls of the third party or obtaining independent review report for the same from CERT-In empaneled security consultant, to ensure it meets Bank's information security requirement.	Pre-Bid Query / Clarification: We request that the Bank permit review of current independent assurance reports/certifications as the primary mechanism for reviewing OEM IT controls. Any direct audit should remain subject to the OEM's standard contractual audit provisions, confidentiality, security, scope and advance-notice requirements. Suggested Clarified Wording / Requested Action: The Bank may review applicable independent third-party assurance reports/certifications covering the hosted service. Where additional audit is required, such audit shall be subject to mutually agreed scope, confidentiality/security restrictions, reasonable advance notice and the OEM's standard contractual audit provisions. A CERT-In empanelled consultant may review evidence made available under these conditions.	Please refer addendum for revised clause
2397	Functional Spec Sheet	Vulnerability Assessment & vulnerability lifecycle Management	1	The proposed solution shall be deployable entirely on-premises and shall not require any cloud-hosted component, external service, or Internet connectivity for its core functionality, scanning, management, reporting, analytics, or product capabilities.	If SIEM, SOAR, Threat Intelligence and other solutions are permitted in a cloud-based model, why is VA-VM specifically mandated to be on-premises? This appears to be an OEM-specific clause. We have several Indian banking customers successfully using our VA solution for years. Request the Bank to kindly relax this clause and allow cloud-based VA-VM deployment.	Please refer addendum for the revised clause
2398		Vulnerability Assessment & vulnerability lifecycle Management	3	The proposed solution shall be software-based and fully deployable on the hardware infrastructure proposed by the Bidder.	If SIEM, SOAR, Threat Intelligence and other solutions are permitted in a cloud-based model, why is VA-VM specifically mandated to be on-premises? This appears to be an OEM-specific clause. We have several Indian banking customers successfully using our VA solution for years. Request the Bank to kindly relax this clause and allow cloud-based VA-VM deployment.	No Change, Please be guided by the RFP
2399		Vulnerability Assessment & vulnerability lifecycle Management	10	The proposed solution shall support deployment across physical, virtual, and containerized environments.	If SIEM, SOAR, Threat Intelligence and other solutions are permitted in a cloud-based model, why is VA-VM specifically mandated to be on-premises? This appears to be an OEM-specific clause. We have several Indian banking customers successfully using our VA solution for years. Request the Bank to kindly relax this clause and allow cloud-based VA-VM deployment.	No Change, Please be guided by the RFP
2400		Vulnerability Assessment & vulnerability lifecycle Management	12	The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and failover capabilities.	If SIEM, SOAR, Threat Intelligence and other solutions are permitted in a cloud-based model, why is VA-VM specifically mandated to be on-premises? This appears to be an OEM-specific clause. We have several Indian banking customers successfully using our VA solution for years. Request the Bank to kindly relax this clause and allow cloud-based VA-VM deployment.	No Change, Please be guided by the RFP
2401		Vulnerability Assessment & vulnerability lifecycle Management	30	The proposed solution should provide predictive risk analysis or exploitability assessment based on vulnerability intelligence and threat context.	If SIEM, SOAR, Threat Intelligence and other solutions are permitted in a cloud-based model, why is VA-VM specifically mandated to be on-premises? This appears to be an OEM-specific clause. We have several Indian banking customers successfully using our VA solution for years. Request the Bank to kindly relax this clause and allow cloud-based VA-VM deployment.	No Change, Please be guided by the RFP
2402		Vulnerability Assessment & vulnerability lifecycle Management	33	The proposed solution shall support deployment and lifecycle management of scanning agents without dependency on cloud-hosted services.	If SIEM, SOAR, Threat Intelligence and other solutions are permitted in a cloud-based model, why is VA-VM specifically mandated to be on-premises? This appears to be an OEM-specific clause. We have several Indian banking customers successfully using our VA solution for years. Request the Bank to kindly relax this clause and allow cloud-based VA-VM deployment.	No Change, Please be guided by the RFP
2403		Vulnerability Assessment & vulnerability lifecycle Management	9	Each scanning engine shall support web application security assessment together with traditional infrastructure vulnerability and configuration/compliance assessment. The solution shall identify vulnerabilities, missing patches, insecure configurations, and compliance deviations, and generate comprehensive reports containing risk severity, evidence of findings, affected assets, and remediation recommendations to support security governance, audit, and regulatory compliance.	Bank has already asked for Application security testing tool, hence this clause needs to be removed under VA-VM.	No Change, Please be guided by the RFP
2404		Vulnerability Assessment & vulnerability lifecycle Management	87	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	This is OEM specific clause. Our tool has capaiblity to provide executive summary along with dashboard. This does not require any AI capabilities to be deployed on-prem. Please confirm if this suffice banks requirement. Prposed change "Proposed solution shall provide critical vulnerability information, including risk/verdict assessment and supporting rationale, along with executive-level vulnerability summaries".	Please refer addendum for revised clause.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2405		Vulnerability Assessment & vulnerability lifecycle Management	91	White-Label Reporting and Approval Workflow: The proposed solution shall support customizable/white-label security assessment reports, including organization-specific branding and configurable report content. The solution shall support role-based maker-checker workflow for report generation, review, approval, and controlled release of finalized reports.	This is OEM specific clause. The widely accepted industry practice is to grant access to users based on role and perform their necessary task. Proposed Change " The platform must support granular RBAC to provision dedicated reporting users/roles. Authorized reporting users must be able to generate, view, schedule, export, and distribute security and vulnerability reports within their assigned asset/data scope, without requiring administrative privileges. Access to reporting data must be governed by user roles and asset/business-unit scope, with appropriate segregation of duties."	Please refer addendum for revised clause.
2406		Vulnerability Assessment & vulnerability lifecycle Management	92	Multi-Tenant Data Isolation: The proposed solution shall support secure multi-tenancy for managed-security/shared-service deployments, providing logical and access-controlled segregation of each customer's assets, credentials, scan configurations, findings, reports, and other security data. APIs and administrative interfaces shall enforce appropriate tenant-level authorization and data isolation.	Does bank need multi-tenancy capabilities? If not, this clause to be removed.	Please refer addendum for revised clause.
2407	35 of 122	XDR	4.13	The goal is to minimize the attack surface by continuously monitoring, updating, and provide compensatory controls for vulnerabilities and exploits in the endpoints	We request to modify this clause as below "The goal is to minimize the attack surface by continuously monitoring, updating, and provide visibility for vulnerabilities and exploits in the endpoints" Justification: The term "visibility" is outcome-focused and technology-agnostic, allowing solutions to detect and report vulnerabilities through various mechanisms (signatures, behavioral analysis, real-time scanning, etc.), whereas "compensatory controls" is overly prescriptive and implies specific mitigation techniques that may not be applicable to all vulnerability types or endpoint environments. Changing to "visibility" maintains the security intent while enabling bidders to propose diverse, fit-for-purpose solutions without unnecessary implementation constraints.	No Change, Please be guided by the RFP
2408	35 of 122		12	The proposed solution must provide protection against malicious AI application tampering on the endpoints	We request to modify this clause as below "The proposed solution must provide protection against malicious applications tampering on the endpoints" Justification:The "AI" qualifier is overly specific and may exclude non-AI malware threats, creating coverage gaps. The broader term "malicious application tampering" aligns with industry-standard endpoint protection language and ensures comprehensive threat protection regardless of the attack vector or technology employed.	No Change, Please be guided by the RFP
2409	36 of 122		15	The proposed XDR solution must provide comprehensive activity data management and search capabilities, including receiving activity data in the form of telemetry, and metadata; feature for automatic query runs and email notifications; threat matching features using Boolean Logic and other criteria; and options to export, import, delete, and share saved search queries.	We request to modify this clause as below: The proposed XDR solution must provide comprehensive activity data management and search capabilities, including receiving activity data in the form of telemetry, and metadata; feature for automatic query runs and email notifications; threat matching features using Boolean Logic and other criteria; and options to export, delete, and share saved search queries. Justification:The "import" functionality is not a core operational requirement for XDR activity data management. The primary requirements are exporting queries for backup/sharing, deleting obsolete queries, and sharing queries among team members—all of which are standard XDR capabilities. Import functionality introduces unnecessary complexity, potential security/governance risks from external query sources, and is not universally supported across commercial XDR solutions, thereby limiting vendor options unnecessarily	No Change, Please be guided by the RFP
2410	36 of 122		22	The solution should offer options to leverage anti-malware and anti-spyware components stored locally on agents, or signatures stored in-the-vendor cloud	From the operational context and use cases for each deployment option, ensuring continuity of threat protection in all connectivity scenarios. By explicitly defining "when offline" (local components) and "when online" (cloud signatures), the clause removes ambiguity regarding the solution's capability to maintain protective coverage during network disconnections while leveraging updated threat intelligence when connectivity is available We request to modify this clause as below "The solution should offer options to leverage anti-malware and anti-spyware components stored locally on agents when offline, or signatures stored in-the-vendor cloud when online."	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2411	36 of 122		29	The solution Device Control capability must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The solution Device Control capability must support Network Devices, USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, time based device control capabilities allowing admin to define the policy specifically for the endpoint operating systems (Windows 10, 11 or higher).	We request to modify the clause as below: The solution Device Control capability must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The solution Device Control capability must support USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, allowing admin to define the policy specifically for the endpoint operating systems (Windows 10, 11 or higher)to allow the devices as required. Justification: Network Devices are typically managed through enterprise network security controls and firewalls rather than endpoint Device Control, and time-based controls create unnecessary operational complexity and maintenance overhead. The modified clause focuses on high-risk local device vectors (USB, Mobile Storage, Bluetooth, Modems) that pose direct security threats to endpoints, while allowing flexibility for organizations to enable specific devices based on business requirements.	No Change, Please be guided by the RFP
2412	37 of 122		43	The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature or through seamless integration with a third-party sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data	We request to amend this clause as below: The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data. Justification: To ensure operational independence and reduce implementation complexity, the organization requires native sandbox functionality built into the core solution rather than relying on third-party integrations, which introduce external dependencies, potential single points of failure, and increase support overhead. This modification mandates that bidders deliver complete sandboxing capability as an integrated component from day 1, ensuring seamless functionality, consistent vendor accountability, and simplified maintenance and support operations without external vendor coordination.	Please refer addendum for revised Clause
2413	38 of 122		57	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	We request to amend this clause as below: The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture or 99.9% availability SLA distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead. Justification: The modification provides architectural flexibility while maintaining the Bank's core availability objective. Not all qualified SaaS vendors employ Active-Active multi-AZ architecture; however, industry-standard 99.9% SLA meets enterprise-grade requirements and enables broader vendor participation without compromising operational resilience. This alternative approach is vendor-agnostic, measurable, and backed by contractual guarantees rather than architectural prescriptions.	Please refer Addendum for revised clause
2414	37 of 122		42	The proposed solution should provide recommended actions to address and mitigate threats detected on endpoints. These remediation suggestions should be informed by forensic data collected from endpoints and detailed analysis performed by the solution to enhance threat response and resolution.	To ensure accurate cost proposals and licensing calculations, please clarify the estimated forensics data volume requirements: a) What is the expected monthly forensics data volume (in GB) that the solution must support? b) What is the planned retention period for forensics data? c) Does this volume include forensics data from all sources (endpoints, servers, cloud workloads, network) or specific sources only? This clarification will enable all bidders to calculate appropriate licensing models and provide consistent cost estimates	Details shall be shared with the successful bidder
2415	54 of 122	Cloud Security	4	The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud envirionment like AWS/Azure/GCP/Meghdoot, AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.	We request to modify this clause as below The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud envirionment like AWS/Azure/GCP/ AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports. Justification: Meghdoot is a comprehensive open-source cloud suite, but bringing it up to PSB requirements demands significant development and integration effort. To be effective, the target cloud environment must be seamless, eliminating the overhead of custom modifications.	Please refer addenudm for revised clause The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud envirionment like AWS/Azure/GCP, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2416	Addition of Point as recommendation	Cloud Security	To be Added in Cloud Security	The proposed solution should also support the File scanning with no limitation on file/object type or size covering application across organisation. This should include but is not limited to Amazon Simple Storage Service (S3), Amazon FSx amd Amanzon Elastic File System.	Benefit to PSB: Comprehensive file scanning eliminates critical security blind spots across the organization's cloud storage infrastructure, ensuring no malware, ransomware, or sensitive data can be inadvertently stored in S3, FSx, or EFS without detection. By removing file type and size limitations, the solution prevents attackers from bypassing scanning through obfuscation or leveraging uncommon formats, while the multi-storage coverage consolidates security posture across diverse AWS storage services under a single unified policy. This provides unified threat visibility, enables regulatory compliance (HIPAA, PCI-DSS, GDPR), prevents data exfiltration, and protects against insider threats and supply chain compromises affecting cloud-stored data—significantly reducing the risk of ransomware attacks, compliance violations, and unauthorized data exposure.	No Change, Please be guided by the RFP
2417	page 30 of 273	Extended Detection & Response (XDR)	5	Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Cloud (SaaS): HA Deployment aligned with the SLA, RTO & RPO (Refer Section 13). Management Console: Deployed at both Primary and Secondary sites	We request to amend this clause as below: Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Cloud (SaaS): HA Deployment aligned with the SLA, RTO & RPO (Refer Section 13). Justification: In Appendix 1A clause 27 under XDR explicitly mention for SaaS "ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead" Though it's a SaaS based the management console cannot be deployed at both primary and secondary sites.	Please refer addendum for revised clause
2418	page 31 of 273	Cloud Workload Protection Platform (CWPP)	13	Cloud (SaaS): Deployment aligned with the SLA, RTO & RPO (Refer Section 13).. Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Management Console: Deployed at both Primary and Secondary sites	We request to amend this clause as below: Cloud (SaaS): Deployment aligned with the SLA, RTO & RPO (Refer Section 13).. Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Justification: For SaaS solution the management console cannot be deployed at banks primary & secondary site	Please refer addendum for revised clause
2419	Page 38 of 122 & Page 38 of 122	XDR	22 to 35	These points are duplicate need to be removed	These points are duplicate need to be removed	No Change, Please be guided by the RFP
2420	29, 35 & 259	Sections 7.2.1, 7.2.4.1(b) & 16.21.2	Section 7.2.1	Deception deployment and high-availability topology (Deception Technology): "Any agent/Enforcer/Deceptor Standalone at DC and HA, N+N, Standalone at DR." Section 7.2.4.1(b): "The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active configuration." Section 16.21.2 (Decoy): "All the inline components of the solution must operate in high availability mode. In the event of any component failure, the system should automatically initiate failovers within seconds, ensuring uninterrupted functionality without requiring manual intervention."	The RFP describes the Bank-side deception components as standalone in Section 7.2.1, point no.- 4, but it is also mentioned HA and N+N. We request the bank to kindly clarify that in case we're deploying the solution on-prem, whether Bank needs the solution in Standalone mode/HA mode/N+N mode. Section 16.21.2 (Decoy), point no.-8, Bank has asked that all the inline components of solution should be in HA mode with automatic failover capability. However, the deception solution is not inline. Hence, we request Bank to clarify if they need the Deception Solution in HA. We request the Bank to add on-prem solution also in addition to Cloud/SAAS+Hybrid.	Please refer addendum for revised clause
2421	45, 261 & 262	Sections 7.3.6.2(2) & 16.21.3 - Deployment and Data Retention	Section 7.3.6.2(2):	Backup, restoration and log-retention requirements "Restore the logs/data from backup for forensic investigation and as per bank requirement without any additional cost." Section 16.21.3: "Duration of the Contract (Monthly Full backup) - Long-Term Storage (LTS) - Entire Duration of the Contract." The RFP further states that applicable Monthly Full Backups shall be migrated to LTS at the Bank's DC & DR and retained for the entire duration of the contract.	We request bank to kindly confirm that if the bank will provide the storage for backup.	No Change, Please be guided by the RFP. Bidder to right size and provide all the required infrastrcuture as per RFP
2422	68	Section 7.7 - On-cloud proposed solution OEM Responsibilities, Point 10	"The OEM shall have valid ISO/IEC 27001 certification and SOC 2 Type II report."	Cloud OEM certification requirement	We request the bank to accept ISO/IEC 27001 or SOC 2 Type II or both.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2423	29, 32 & 35	Sections 7.2.1, 7.2.3 and 7.2.4.1(b)	Section 7.2.1 (Deception Technology): "Cloud (SaaS) + Hybrid" Section 7.2.3: "The solution shall be hosted through a Cloud Service Provider (CSP), either fully as a SaaS service or through a combination of CSP-hosted and Bank-hosted components." Section 7.2.4.1(b): "Deception Technology: The core Deception platform shall be deployed in the	Responsibility for providing the Cloud/SaaS environment	7.2.4.1(b) We request the bank to kindly add the on-prem implementation option also for the core component of the Deception Solution.	Please refer addendum for revised clause
2424	35 & 91	Sections 7.2.4.1(b) and 7.18.1 - Compute Infrastructure, Point 1	Section 7.2.4.1(b): "Deception Technology: The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active configuration. The Cloud/SaaS deployment shall be aligned with the applicable SLA, RTO and RPO requirements."	Hardware and VM infrastructure for Bank-hosted deception components	We request the bank to kindly add the on-prem implementation option also for the core component of the Deception Solution.	Please refer addendum for revised clause
2425	84	Breach and Attack Simulation (BAS)	Sl. No. 1 - Technical Specification	The solution should simulate Ransomware Attacks	Rationale for change: The clause as drafted is a single unqualified statement that every bidder in this category will mark compliant, so it cannot differentiate responses against the 10 marks allotted. It also does not define what constitutes a ransomware simulation. A ransomware validation exercise is only meaningful to the Bank if the platform reproduces the tradecraft ransomware operators actually use, including vulnerable driver loading to terminate endpoint protection, and does so without causing damage on production assets. The Bank is requested to replace the clause with testable criteria covering safe execution of destructive behaviours, deterministic cleanup, and kernel-level attack testing. Proposed modified clause: The proposed solution must execute structurally authentic attacks with destructive elements neutralised, and must be able to trigger destructive-technique detections without the harmful action (for example, testing volume shadow copy deletion detection without deleting the volume shadow copy). It must provide deterministic cleanup mechanisms, safe for execution on production assets, including backup, restore, and removal of all artifacts across: a. File b. Registry c. Service	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2426	84	Breach and Attack Simulation (BAS)	Sl. No. 3 - Technical Specification	The ability to simulate infiltration techniques for breaching a network or infecting a host	Rationale for change: "Infiltration techniques" is undefined and cannot be evaluated objectively. Initial access is the stage at which the Bank's email gateway, secure web gateway and web application firewall are tested, and current adversary tradecraft delivers initial access through container formats such as ISO, IMG, MSI, LNK and ZIP, followed by execution that avoids system interpreters in order to bypass AMSI, script block logging and constrained language mode. A clause that names these delivery and execution requirements allows the Bank to compare bidders on demonstrable capability rather than on a general claim. Proposed modified clause: The proposed solution must dynamically generate container-format payloads including ISO, IMG, MSI, LNK, and ZIP variants containing executables, shortcuts, or DLL hijack chains, and deliver them via uniquely generated URLs per simulation to comprehensively validate email gateway, secure web gateway, and WAF filtering against modern initial-access techniques such as ISO-LNK-DLL chains. The simulation agent must execute malicious behaviours and adversary techniques without reliance on system interpreters including PowerShell, CMD, BASH, or SH, validating control effectiveness against modern adversary tradecraft that increasingly avoids interpreter-based execution to bypass AMSI,	No Change, Please be guided by the RFP
2427	84	Breach and Attack Simulation (BAS)	Sl. No. 6 - Technical Specification	The solutions should test Security Operations Center (SOC) detection capability of bank by simulating multi-chained payloads with advanced evasion methods including DLL Hijacking, Process Injection, and PPID spoofing for breaching and infiltrating the network.	Rationale for change: The clause names only three evasion techniques and does not state that they must be executed as real behaviours on the asset rather than logged as simulated steps. SOC detection validation succeeds or fails on two things the clause does not capture: whether the payload natively performs modern evasion against the deployed control stack, and whether each technique is available in multiple procedure variants, since a detection that catches one implementation of LSASS credential dumping routinely misses six others. The Bank is requested to expand the clause so that detection coverage is validated across the attacker variant space. Proposed modified clause: The simulation payload execution must natively perform the following techniques as executed behaviours against the deployed control stack: a. EDR unhooking (NTDLL unhooking, direct and indirect syscalls) b. Reflective DLL injection c. Process hollowing d. PPID spoofing e. Command-line argument spoofing f. Fileless in-memory execution For each in-scope MITRE ATT&CK technique, the proposed	No Change, Please be guided by the RFP
2428	84	Breach and Attack Simulation (BAS)	Sl. No. 7 - Technical Specification	The solution should have the ability to create custom use cases / simulations attacks according to bank's requirement.	Rationale for change: As drafted the clause is satisfied by a script upload field or by a vendor professional services engagement, both of which leave the Bank dependent on the OEM for every new scenario and carry recurring cost. For the Bank's own security team to build scenarios for proprietary applications and internal workflows, the clause should require a user interface driven attack creator with named configurable parameters. Proposed modified clause: The proposed solution must provide a UI-driven attack creator enabling customer security teams to design custom multi-stage simulations with configurable name, description, MITRE category, execution privileges (User/Admin), payload type (DLL/EXE/Service/ISO/MSI/LNK), and chained secondary behaviours supporting organisation-specific scenario testing for proprietary applications, internal workflows, and bespoke attack hypotheses.	No Change, Please be guided by the RFP
2429	84	Breach and Attack Simulation (BAS)	Sl. No. 8 - Technical Specification	The solution must allow the execution of simulations on multiple agents simulataneously. An attack chain must be executed on multiple endpoints agents at the same time to provide unique attack specific insights across the deployed agents in the organisation.	Rationale for change: The clause states the requirement for simultaneous execution but does not exclude sequential execution presented as a single campaign, which is how several solutions in this category operate. It also does not address the operational prerequisites for running simulations across a bank-scale estate: the agent must be deployable at scale through Group Policy or golden image, must run silently so that branch and business users are not alerted or disrupted, and must update centrally without re-imaging or desk visits. The Bank is requested to make both the concurrency model and the deployment model explicit. Proposed modified clause: The proposed solution must execute a single coordinated attack campaign across multiple agents, business units, and geographies simultaneously, not sequentially (i.e. One Kill chain, run on multiple Endpoint Targets at the same time), producing independent per-agent evidence consolidated into a unified campaign report. Solutions that walk through agents one-by-one cannot realistically validate enterprise-scale concurrent compromise scenarios. The simulation agent must be a lightweight software package suitable for enterprise mass-deployment via Group Policy Object (GPO), golden image baking, or standard endpoint management tooling, requiring no per-host configuration post-installation.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2430	84	Breach and Attack Simulation (BAS)	Sl. No. 11 - Technical Specification	The solution should support technical integrations with bank's existing solutions (e.g., SIEMs, ticketing systems, log management, Firewalls, automation/orchestration, analytics solutions, threat intelligence solutions, etc.)	Rationale for change: "Should support technical integrations" is unverifiable and is routinely answered with roadmap commitments or bespoke development quoted after award. For closed-loop validation, where a simulation result is correlated against the alert raised in the Bank's SIEM and a ticket is created automatically, the Bank needs a documented API, automation tooling and pre-built connectors available at the time of bid. The Bank is requested to make the integration requirement specific and verifiable. Proposed modified clause: The proposed solution must expose a RESTful API with publicly available OpenAPI documentation, provide an open-source CLI and SDK for automation, and ship pre-built integrations with major SIEM, SOAR, ITSM, EDR, firewall, and email gateway vendors to enable closed-loop validation of alerts, automated ticket creation, and detection correlation.	No Change, Please be guided by the RFP
2431	30	RFP - 7.2 Solution & Services Deployment Model and Their HA Requirement 7.2.1 Solutions – Master Deployment Matrix	6. Network Detection & Response (NDR)	Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Management Console: Deployed at both DC and DR	Different NDR solution works on different redundancy deployment methodology (I.e Active - Active or Active - Passive). Request bank to modify the clause as: Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active/Passive at DC and HA, N+N, Active-Active/Passive at DR. Management Console: Deployed at both DC and DR	Please refer addendum for revised clause
2432	45	RFP - Scope of Work 7.3.5 Network detection and response (NDR)	7.3.5.1 Modules, Architecture & Deployment:	Pt 2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Generally NDR solutions are deployed with sole purpose of doing network analysis, threat detection & response and does not have native 2FA capability, so request bank to remove this point. As an alternate as proposed in same point, proposed NDR solution can be integrated with bank's existing MFA solution.	Please refer addendum for the revised clause
2433	49	RFP - Scope of Work 7.3.10 Application security testing Tool	7.3.10.1 Modules, Architecture & Deployment:	Pt 2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Generally AST solutions are deployed with sole purpose of scanning the source code, web, api etc and does not have native 2FA capability, so request bank to remove this point. As an alternate as proposed in same point, proposed AST solution can be integrated with bank's existing MFA solution.	No Change, Please be guided by the RFP
2434	110	RFP - 10.2 Eligibility Evaluation Criteria	OEM Evaluation Criteria	Pt 19. The proposed OEM SIEM Solution with a minimum capacity of 30,000 EPS or 1.2 TB/day shall have been successfully implemented on cloud in one (1) in India.	For wider participation, we request bank to amend the clause as: The proposed OEM SIEM Solution with a minimum capacity of 5,000 EPS or.2 TB/day shall have been successfully implemented on cloud in any one (1) Govt/PSU customer in India. OR The proposed OEM SIEM Solution with a minimum capacity of 10,000 EPS or.4 TB/day shall have been successfully implemented on cloud in one (1) in India.	Please refer addendum for revised clause.
2435	112	RFP - 10.2 Eligibility Evaluation Criteria	OEM Evaluation Criteria	Pt 20. The proposed OEM solution should have been implemented in at least one BFSI is to be submitted for the following solutions: NDR	For wider participation, we request bank to amend the clause as: The proposed OEM solution should have been implemented in at least one BFSI / Govt is to be submitted for the following solutions: NDR	Please refer addendum for the revised clause
2436	260	RFP - 16.21.2 Volumetrics- Solution-wise Requirements	12. Application Security Testing Tool	All the inline components of the solution must operate in high availability mode. In the event of any component failure, the system should automatically initiate failovers within seconds, ensuring uninterrupted functionality without requiring manual intervention.	Application Security Testing as a technology in general works at developemnt/pre-production/UAT stage only. And hence as a solution there is no need of high availability mode. Same has already been updated in this RFP (as solution is asked in standalone at both DC & DR). So, request bank to deleted this clause.	No Change, Please be guided by the RFP. The bidder must design the solution to fully comply with the RFP requirements, ensuring that in case of a failover, the system meets the defined SLA for availability, RTO, and RPO. The bidder is required to adhere to the deployment requirements outlined in the RFP when designing and proposing the solution architecture.
2437	40	APPENDIX 1A Functional Compliance Sheet (Solutions)	Network Detection & Response (NDR)	Pt 8. Proposed solution should generate a root cause analysis, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets.It should provide a platform for easier investigation like visual graphical view and timeline of the attack and it should support tagging of MITRE tactics, techniques and procedures used by the attacker in alerts and incidents.	We reqeust bank to amend the clause: Proposed solution should generate a root cause analysis / incident management, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets.It should provide a platform for easier investigation like visual graphical view and timeline of the attack and it should support tagging of MITRE tactics, techniques and procedures used by the attacker in alerts and incidents.	Please refer addendum for the revised clause
2438	40	APPENDIX 1A Functional Compliance Sheet (Solutions)	Network Detection & Response (NDR)	Pt 13. The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	As bank has asked for on-premise solution for NDR, on the contrary, this clause asks for cloud-native SAAS ask. So, we kindly request bank to delete this clause.	Please refer Addendum for revised clause
2439	42	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 3. The solution must be able to analyse a wide array of programming languages including Java,.Net, C/C++, Objective-C, Android, PHP, COBOL, Ruby, Swift, HTML 5, Scala, APEX, TypeScript, Go, Kotlin and ABAP etc but not limited to these alone	Considering the future requirements of AI in Secure Code Development and most of the development is moving towards AI generated code using AI supported languages. So it is very important for bank to have coverage around this as well and will recommend to incorporate AI supported languages like "R, Ada, Solidity, Bash, Groovy, Rust, Perl", but not limited to these alone.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2440	42	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 24. Solution should support Machine learning and Analysis based on the archived results	ML capability is important, but it is very important to have coverage around AI based code as well. And will recommend bank to consider: The solution should have the capability to scan AI generated code. The solution should be able to integrate with AI coding agent via MCP	No Change, Please be guided by the RFP
2441	43	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 32. The solution should be able to support Composition Analysis: Identify the opens source components used in the application. Vulnerabilities & outdated version Licensing risk associated with the components	Bank is looking for Software composition analysis and asked for identifying the open source component and licensing risk. But this limited information is not enough for bank to secure themselves with rapidly increasing supply chain attacks and we will highly recommend to consider following as well: SCA system must catalogue open source components from Maven, NPM, and Nuget. SCA system has to be able to generate a Bill of Materials for an application. Solution should have the ability to continuously monitor the scanned components & notify if there are any zero day attacks without performing the rescan. Solution should Catalog, Store, and Audit SBOMs (both cycloneDx & SPDX) generated for in-house developed software applications and COTS applications.	No Change, Please be guided by the RFP
2442	30	7.2 Solution & Services Deployment Model and Their HA Requirement 7.2.1 Solutions – Master Deployment Matrix	Sl. No. 8	Vulnerability assessment (VA) & vulnerability lifecycle management Bank Location: Standalone at DC and Standalone at DR. Management Console: Deployed at both DC and DR	Requesting clarifications if standalone management console in DR will be live or will be on standby ?	Please refer addendum for revised clause
2443	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 1 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall be deployable entirely on-premises and shall not require any cloud-hosted component, external service, or Internet connectivity for its core functionality, scanning, management, reporting, analytics, or product capabilities.	Requesting change to: The proposed solution shall be deployable entirely on-premises or hosted on MeitY cloud or Meity empanelled cloud environment. No data shall be shared with the platform/cloud outside India geolocation.	Please refer addendum for the revised clause
2444	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 3 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall be software-based and fully deployable on the hardware infrastructure proposed by the Bidder.	Requesting change to: The proposed solution shall be software-based and fully deployable on the hardware infrastructure or should support hybrid- on-premise architecture with management-console or scanners on on-premise and analytics components on MeitY/MeitY-emapanneled cloud proposed by the Bidder.	No Change, Please be guided by the RFP
2445	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 9 of Vulnerability Assessment & vulnerability lifecycle Management	Each scanning engine shall support web application security assessment together with traditional infrastructure vulnerability and configuration/compliance assessment. The solution shall identify vulnerabilities, missing patches, insecure configurations, and compliance deviations, and generate comprehensive reports containing risk severity, evidence of findings, affected assets, and remediation recommendations to support security governance, audit, and regulatory compliance.	Requesting to confirm that if DAST specs are specifically provided for web-application's VAPT, then what is the scope of "web-application" scanning in this spec? Also requesting to share the total number of web-applications considered in the scanning scope.	No Change, Please be guided by the RFP
2446	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 18 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall support both active and passive asset discovery and vulnerability assessment/scanning.	Requesting change to: The proposed solution shall support both active and/or passive asset discovery and vulnerability assessment/scanning.	No Change, Please be guided by the RFP
2447	48	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 27 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall support both active and passive techniques for vulnerability detection, where applicable.	Requesting change to: The proposed solution shall support both active and/or passive techniques for vulnerability detection, where applicable.	No Change, Please be guided by the RFP
2448	48	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 33 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall support deployment and lifecycle management of scanning agents without dependency on cloud-hosted services.	Requesting change to: The proposed solution shall support deployment and lifecycle management of scanning agents.	No Change, Please be guided by the RFP
2449	48	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 34 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall assess Active Directory security posture and identify misconfigurations, privilege risks, insecure policies, and exposure of critical directory services.	Requesting to clarify that this spec is already addressed in IDTR then what is the requirement of it in VM solutin?	No Change, Please be guided by the RFP
2450	49	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 74 of Vulnerability Assessment & vulnerability lifecycle Management	The solution shall support offline signature and plugin updates for deployment in isolated or air-gapped environments.	Requesitng to remove this spec because if the cloud-based solution is offered and where cloud is hosted on MeitY cloud or MeitY empanneled cloud then questions related to air-gap environment doesn't arise.	No Change, Please be guided by the RFP
2451	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 81 of Vulnerability Assessment & vulnerability lifecycle Management	The solution shall support password-protected and/or digitally signed reports with configurable retention and archival.	Requesting change to: The solution must support secure, encrypted report distribution (including native PGP encryption) and enforce strict role-based access controls (RBAC) for report viewing. Additionally, the platform must provide configurable cloud-based data retention policies alongside automated options to archive historical scan data and reports to external storage	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2452	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 87 of Vulnerability Assessment & vulnerability lifecycle Management	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	Requesting change to: The solution must provide AI-generated risk summaries and plain-language vulnerability briefs that automatically fuse asset criticality, technical findings, and real-world threat telemetry (such as CISA KEV and EPSS data) to streamline IT triage. If cloud analytics are utilized to run these machine learning models, the solution vendor must guarantee that all data is isolated within dedicated, bank-authorized cloud regions, employing strict data privacy frameworks that ensure source code, credentials, and raw scan parameters are explicitly excluded from public AI training models or multi-tenant public AI services	Please refer addendum for revised clause
2453	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 88 of Vulnerability Assessment & vulnerability lifecycle Management	Unified, correlated findings intelligence. Every scanning engine — across web, API, network and host, cloud, containers, mobile, source code, device configuration and identity — reports into a single normalized findings model..	Requesting clarification on why unified reporting is asked as the ASM, VM, DAST solutions are considered separately.	No Change, Please be guided by the RFP
2454	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 90 of Vulnerability Assessment & vulnerability lifecycle Management	Mobile Application Security Testing: The proposed solution shall support static security analysis of Android and iOS mobile application packages, including APK/AAB and IPA formats, and shall provide security assessment mapped to recognized mobile application security standards and methodologies such as OWASP MASVS and MASTG.	Requesting clarification for the spec as the ask is for DAST or MAST solution.	No Change, Please be guided by the RFP
2455	87	Anti Phishing Services	17.1	Solution should detect at the earliest point in the attack, post initial compromise as the attacker is first attempting to move laterally and escalate privilege.	Since this section is focused on Anti-Phishing, we understand that the objective is to identify suspicious activity following a successful phishing or account-compromise event. Network-level lateral movement and deception capabilities may be addressed by other security controls. We request the Bank to clarify whether this clause may instead focus on early post-compromise user activity visibility for the Bank's most critical users. " The solution should support early identification and investigation of suspicious user activities associated with potential account compromise following phishing or other email-originated attacks, with enhanced user activity monitoring for up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles."	Please refer to the relevant Addendum for updated specfications
2456	87	Anti Phishing Services	17.4	Solution must provide robust supply chain and AI/ML-driven contact chain analysis capabilities to identify and defend against socially engineered, impersonated, or BEC attacks.	As compromise of trusted suppliers and partners is an important source of BEC and phishing risk, we request the Bank to clarify whether the existing supply-chain requirement should explicitly include behavioural analysis of supplier/partner communication patterns to identify attacks originating from compromised trusted accounts. " Solution must provide robust supply-chain and AI/ML-driven contact-chain and behavioural analysis capabilities to identify and defend against socially engineered, impersonated or BEC attacks, including threats originating from compromised or impersonated supplier/partner accounts."	Please refer to the relevant Addendum for updated specfications
2457	87	Anti Phishing Services	18	Solution must proactively analyze suspicious URLs using dynamic/behavioral analysis to prevent the spread of malware and other threats.	The RFP separately addresses URL analysis and post-delivery remediation. We request clarification whether these requirements are intended to provide continuous protection throughout the email threat lifecycle, including pre-delivery analysis, click-time URL protection and post-delivery detection/remediation. " Solution must provide continuous protection across the email threat lifecycle, including pre-delivery threat detection, real-time/click-time inspection of suspicious URLs, and post-delivery detection and automated remediation of threats that are subsequently determined to be malicious."	Please refer to the relevant Addendum for updated specfications
2458	88	Anti Phishing Services	19.7	Solution must be able to offer a comprehensive portal that allows users to access information and metadata on events/incidents, facilitating network threat forensics for thorough investigation and analysis of potential security breaches or incidents.	To strengthen investigation of phishing-led incidents involving executives and other critical users, we request clarification whether the existing forensic portal requirement may also include contextual user and endpoint activity for a limited population of Bank-identified critical/high-risk users. " Solution must offer a comprehensive investigation portal providing information and metadata on events/incidents for forensic analysis. For up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, the portal should additionally provide contextual user and endpoint activity, including relevant application, file and user-action details, to support investigation of potential phishing-led compromise."	Please refer to the relevant Addendum for updated specfications
2459	88	Anti Phishing Services	19.9	Solution must empower security operations and incident responders to automate the identification, remediation, and sharing of phishing threats, streamlining the process of detecting, addressing, and disseminating information about potential phishing attacks for improved response and mitigation.	To improve SOC investigation efficiency, we request clarification whether the existing phishing identification and remediation requirement should include centralized attack context showing why a message was identified as malicious, the users targeted, associated threat indicators and remediation status. " Solution must empower security operations and incident responders to automate identification, investigation, remediation and sharing of phishing threats, and should provide centralized contextual visibility into the users targeted, associated threat indicators, detection rationale, attack characteristics and remediation actions."	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2460	88	Anti Phishing Services	19.1	Solution must provide incident responders with real-time analytics and visibility into email-based attacks targeting the organization.	Email-based attacks against executives and privileged users may require additional context after delivery to determine whether a targeted user has subsequently performed suspicious activity. We request the Bank to clarify whether real-time investigation visibility may include relevant user activity context for up to 100 Bank-identified critical/high-risk users. " Solution must provide incident responders with real-time analytics and visibility into email-based attacks targeting the organization. For up to 100 Bank-identified critical/high-risk users, the solution should additionally provide contextual visibility into suspicious user activities associated with potential phishing or account compromise, including relevant user, endpoint, application and file activity."	Please refer to the relevant Addendum for updated specfications
2461	88	Anti Phishing Services	19.23	Solution must have simplicity of evaluation and additional visibility into internal traffic and other communication channels can reduce risk, and baseline user activity to detect suspicious behavior.	The existing clause already seeks baselining of user activity to detect suspicious behaviour. We request the Bank to clarify the intended depth and scope of this capability and whether enhanced monitoring may be applied to a focused population of up to 100 Bank-identified critical/high-risk users, where deeper visibility provides the greatest security value. " Solution must provide additional visibility into relevant internal activity and communication channels to reduce risk and baseline user activity to detect suspicious behaviour. Enhanced user and data activity monitoring should be provided for up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, with configurable detection policies for suspicious, anomalous or policy-violating activities."	Please refer to the relevant Addendum for updated specfications
2462	90	Anti Phishing Services	19.7	Solution must provide protection against harassment mail and mitigate the risks associated with emails from unknown senders specifically for executives or VIPs, safeguarding them from potential threats and ensuring their email communication remains secure.	Since this clause already provides enhanced protection for executives/VIPs, we request the Bank to clarify whether such enhanced protection should extend beyond receipt of suspicious email to investigation of risky user and data activities that may occur following phishing or account compromise, for a limited set of the Bank's most critical users. "Solution must provide protection against harassment mail and mitigate risks associated with emails from unknown senders specifically for executives or VIPs. For up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, the solution should additionally provide enhanced visibility into risky user and data activities following suspected phishing or account compromise, including relevant file movement, web/upload activity, removable-media activity and other supported data-transfer channels."	Please refer to the relevant Addendum for updated specfications
2463	52	Idendity Threat Detection and Response (ITDR)	1.7	Detect and respond to active threats with high fidelity (low false positives and false negatives).	The Bank has separately specified a comprehensive deception platform for detection of active attacker activity, reconnaissance and lateral movement. We understand that the intent of this clause within ITDR is therefore to complement those controls with focused monitoring of the Bank's most critical identities. Considering that enhanced user-activity monitoring is most relevant for high-risk personnel such as executives, privileged users and other critical users, we request the Bank to kindly clarify whether this requirement may be read as follows: " Identity Threat Detection Solution should provide high-fidelity detection and response for risky or anomalous user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, to identify activities associated with careless, malicious or compromised users. "	No Change, Please be guided by the RFP
2464	52	Idendity Threat Detection and Response (ITDR)	1.8	Provide contextual information—who, what, when and how—to inform all stages of the attack chain.	The Bank has already sought attack-lifecycle visibility under the separate deception requirements. For ITDR, we understand that additional value would be derived from detailed user-centric context for the Bank's most critical identities, enabling investigation of risky activity performed by such users. We request the Bank to kindly clarify whether this requirement may be read as follows: " Identity Threat Detection Solution should provide contextual information—who, what, when, where and how—around risky user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, to support investigation and response."	No Change, Please be guided by the RFP
2465	52	Idendity Threat Detection and Response (ITDR)	1.9	Provide deep insights into both the potential and used privilege escalation and lateral movement steps in an attack.	Privilege escalation and lateral-movement visibility is already substantially addressed under the separately specified deception solution, including attacker lifecycle visibility, MITRE ATT&CK mapping, deceptive attack paths and detection of lateral movement. To avoid duplication while retaining complementary investigation capability for high-risk identities, we request the Bank to kindly clarify whether this requirement may be read as follows: "Identity Threat Detection Solution should provide deep insights into activities performed by up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, covering application usage, file and data movement, endpoint activity and other risky behaviours to support investigation of compromised, malicious or negligent user activity."	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2466	52	Idendity Threat Detection and Response (ITDR)	2.9	Detect all types of attack vectors including pre-attack reconnaissance, zero-day attacks, privilege escalation prevention, lateral movement and data theft.	Pre-attack reconnaissance, lateral movement, malware/attack behaviour and attacker lifecycle visibility are already covered under the Bank's separate deception specifications. We understand that the complementary requirement under ITDR should focus on identity/user risk and potential data-loss activity for the Bank's most critical users rather than duplicate the deception control. We request the Bank to kindly clarify whether this requirement may be read as follows: " Identity Threat Detection Solution should detect risky user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, including suspicious application usage, unauthorized access or movement of sensitive information, removable-media activity, web-based transfer, cloud synchronization and other potential data-exfiltration activities."	The Clause is applicable only to idendity related threat vector only. The volumetrics is provided in the RFP and should be complied
2467	52	Idendity Threat Detection and Response (ITDR)	2.10	Detect multiple attacks simultaneously.	We understand the intent is to ensure that the solution is not restricted to investigation of a single event at a time. Since active attacker detection is separately covered by the deception solution, we request that this clause be clarified in terms of concurrent monitoring and investigation of risky activities across the Bank's designated critical-user population: "Identity Threat Detection Solution should be capable of detecting and investigating multiple risky user and data activities simultaneously across up to 100 critical/high-risk users and their monitored endpoints."	No Change, Please be guided by the RFP
2468	52	Idendity Threat Detection and Response (ITDR)	3.2	Provide unified presentation of both source- and target-based telemetry data in a timeline view.	The Bank has separately specified end-to-end attacker visibility and behavioural analysis under the deception solution. For ITDR investigations involving critical identities, a chronological user-activity view would provide complementary evidence of actions performed by the user. We request the Bank to kindly clarify whether the requirement may be read as follows: " Identity Threat Detection Solution should provide a unified chronological timeline of user- and endpoint-based activity telemetry for up to 100 critical/high-risk users identified by the Bank to support investigation of risky or suspicious user activity."	No Change, Please be guided by the RFP
2469	52	Idendity Threat Detection and Response (ITDR)	3.3	Correlate identity-related telemetry from relevant source and target systems to identify and investigate identity compromise, privilege escalation, credential abuse and lateral movement.	Privilege escalation and lateral-movement detection are already addressed through the separately specified deception controls. To provide complementary investigation capability for the Bank's highest-risk identities, we request the Bank to clarify whether this clause may focus on correlation of user, endpoint, application and data activity for the designated critical-user population: " The solution shall support correlation of user, endpoint, application and data-activity telemetry for up to 100 critical/high-risk users identified by the Bank to identify and investigate suspicious user behaviour, sensitive-data movement, policy violations and potential data-exfiltration activities."	No Change, Please be guided by the RFP
2470	52	Idendity Threat Detection and Response (ITDR)	3.4	Integrate with compatible endpoint/extended detection solution to capture screen recordings or screenshots during active attacker sessions as advanced forensic evidence.	The Bank has separately specified attacker-session and forensic visibility through the deception platform. Within ITDR, we understand that visual evidence is intended to strengthen investigation of high-risk user activity. We request the Bank to kindly clarify whether the requirement may be read in an outcome-based manner for the designated critical-user population: " The Identity Threat Detection Solution should support screenshots, screen capture or equivalent visual evidence of relevant activity for up to 100 critical/high-risk users during suspicious or high-risk user sessions, as part of forensic investigation and evidence collection."	Please refer addendum for revised clause.
2471	52	Idendity Threat Detection and Response (ITDR)	3.5	Integrate with compatible network detection solution to support collection of PCAP data for network-level incident visibility.	The requirement for PCAP is network-centric and does not directly relate to identity posture or focused user-activity monitoring. Further, the Bank's separate deception specifications already require high-interaction decoys, recording of attacker activities, traffic/behaviour visibility, forensic investigation and integration with network/security technologies. To avoid duplication of network-level forensic controls across two solution categories, we request the Bank to kindly delete this clause from the ITDR section.	Please refer addendum for revised clause.
2472	52	Idendity Threat Detection and Response (ITDR)	3.6	Push incident data into SIEM/XDR or SOAR technologies via integrations for improved incident management.	We understand that the objective is to ensure relevant ITDR alerts and investigation context are available to the Bank's SOC ecosystem. For the enhanced monitoring of designated critical users, we request the Bank to kindly clarify whether alerts and activity information may be shared through supported integrations or APIs as follows: " Identity Threat Detection Solution should make alerts and relevant incident/activity data for the monitored critical-user population available to SIEM/XDR, SOAR or other supported security platforms through integrations or APIs for improved incident management."	The proposed solution hould be integrated with SIEM/XDR or SOAR technologies for sharing the incident data via supported integrattion or APIs
2473	52	Idendity Threat Detection and Response (ITDR)	3.7	As part of forensic data collection, include detailed attack path information including protocols leveraged during the attack.	Detailed attack-path and attacker-behaviour visibility is already sought under the separate deception specifications, including deceptive attack paths, MITRE ATT&CK mapping and forensic investigation. To avoid overlap while retaining complementary evidence for investigations involving the Bank's critical identities, we request the Bank to kindly clarify whether the requirement may be read as follows: " Identity Threat Detection Solution should, as part of forensic data collection for up to 100 critical/high-risk users, include detailed user-activity information such as applications used, files accessed, data movement, destination channels and other relevant endpoint activity associated with the incident."	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2474	52	Idendity Threat Detection and Response (ITDR)	3.8	Collect user and computer information from Active Directory as part of forensic data gathering to enhance context and assess risk exposure.	We understand that directory information is required to enrich investigations with user and computer context. We request the Bank to clarify that enterprise identity context may be maintained for the overall identity population, while detailed endpoint/user-activity telemetry may be applied to the Bank's designated critical-user population: " Identity Threat Detection Solution should use relevant user and computer identity information to enhance forensic context and risk assessment, and should correlate such context with detailed endpoint/user-activity telemetry for up to 100 critical/high-risk users identified by the Bank."	Please refer addendum for revised clause
2475	52	Idendity Threat Detection and Response (ITDR)	3.9	Detect an adversary's attempt to move laterally toward key assets using as many Windows, Mac or Linux hosts as possible without requiring a persistent agent.	The Bank's separate deception specifications expressly require detection of lateral movement, reconnaissance, credential theft and malicious activity using agentless and/or agent-based deception techniques across the enterprise. The present clause therefore duplicates a capability already being procured under the Deception section. To avoid overlapping scope and duplicate controls, we request the Bank to kindly delete this clause from the ITDR section.	Please refer addendum for revised clause
2476	52	Idendity Threat Detection and Response (ITDR)	3.10	Collect AD user/computer information for forensic context and detect at the earliest point post initial compromise as the attacker first attempts lateral movement and privilege escalation.	Early detection of lateral movement and privilege-escalation activity is substantially covered under the Bank's separate deception requirements. To retain a complementary identity/user-risk objective without duplicating the deception scope, we request the Bank to kindly clarify whether this clause may focus on early detection of risky activity among the designated critical-user population: " Identity Threat Detection Solution should use relevant identity context and detect risky user behaviour at the earliest possible point for up to 100 critical/high-risk users, based on monitored endpoint activities and configured detection policies, enabling investigation and response before such activity results in significant data loss or business impact."	Please refer addendum for revised clause
2477	52	Idendity Threat Detection and Response (ITDR)	3.11	Collect AD user/computer data during forensic gathering while ensuring all deception techniques remain hidden from legitimate users.	The requirement to ensure deception techniques remain hidden from legitimate users is inherently a deception-platform capability. The Bank has already included comprehensive deception requirements covering lures, breadcrumbs, fake credentials, deceptive assets, attacker engagement and techniques designed to remain undetected by attackers. We therefore request the Bank to kindly delete this clause from the ITDR section to avoid duplication.	Please refer addendum for revised clause.
2478	2	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	10	OEM shall ensure compliance of the complete proposed solution & platform with RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and all applicable regulations throughout the contract period.	We request the Bank to clarify that the OEM is required to maintain applicable security, privacy and regulatory controls relevant to the services provided and furnish available compliance/assurance documentation, while the overall regulatory compliance obligation of the Bank remains subject to the Bank's deployment, configuration and usage of the service. " OEM shall maintain security, privacy and compliance controls applicable to the proposed hosted service and shall provide available independent assurance reports, certifications and relevant compliance documentation to support the Bank's obligations under applicable RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and other applicable regulatory requirements."	Please refer addendum for revised clause
2479	2	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	20	The Service uptime agreement for the proposed solution on cloud should have monthly uptime commitments and have transparent monthly credit calculations in case of uptime not being met for any services.	We understand that published/contracted OEM hosted-service SLA commitments and corresponding service-credit methodology shall meet this requirement. Kindly confirm.	No Change, Please be guided by the RFP
2480	3	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	29	Solution provider should provide the design and process for data deletion in the scope of an independent audit and that the operational effectiveness of these controls is tested. The report for the same should be submitted to bank as and when asked by bank.	For a globally operated hosted security service, control effectiveness is generally evidenced through independent assurance reports such as SOC 2 Type II and documented data-retention/deletion controls. We request the Bank to permit such independent assurance documentation instead of requiring a separate bespoke data-deletion audit report. " Solution provider shall maintain documented secure data-retention and deletion controls. Compliance may be demonstrated through applicable independent third-party assurance reports/certifications (such as SOC 2 Type II or equivalent) and documented data-retention/deletion policies made available subject to OEM confidentiality requirements."	Please refer addendum for the revised clause
2481	4	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	41.3	Independent audit for testing effectiveness of secure data removal, such that data is rendered permanently inaccessible. (Including any backup or distributed online media).	We request the Bank to accept independently audited secure deletion and media-management controls, together with documented retention/deletion periods, rather than requiring a customer-specific audit of all backup and distributed media. " The OEM shall maintain secure data deletion, media handling and backup-retention controls designed to render customer data inaccessible in accordance with documented retention schedules. Effectiveness may be evidenced through independent assurance reports such as SOC 2 Type II/ISO 27001 or equivalent and relevant OEM security/privacy documentation."	Please refer addendum for the revised clause
2482	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	47.2	Bank shall have an option to implement 'Bring Your Own Key' as and when required.	The proposed service protects data at rest and in transit using strong encryption; however, customer-managed infrastructure encryption keys are not a standard capability of the hosted anti phishing service. We request deletion of the BYOK requirement, or acceptance of OEM-managed enterprise-grade encryption and key-management controls. " Requested Action: Delete the BYOK requirement. Alternatively: 'Data processed/stored by the hosted service shall be protected using industry-standard encryption in transit and at rest, with secure OEM-managed key-management controls subject to independent security assurance.'"	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2483	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	49	Web Application Firewall shall be implemented on the cloud for Web based applications. WAF application signature should be updated and reviewed regularly. The Report shall be submitted to bank on a periodic interval.	Since the proposed platform is an OEM-managed hosted security service, underlying WAF technology, signatures and configurations form part of the OEM's internal security architecture and may not be exposed as customer-specific reports. We request the Bank to accept periodic VAPT/penetration-test assurance or equivalent independent security assessment evidence covering the hosted application instead of WAF signature reports. " The hosted web application/platform shall be protected through appropriate application-security controls. The OEM shall conduct periodic vulnerability assessment and penetration testing/security assessments and, subject to confidentiality restrictions, provide an executive summary/attestation or applicable independent assurance evidence to the Bank on request. Customer-specific WAF signature reports shall not be mandatory."	Please refer addendum for revised clause
2484	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	52	The systems in cloud infrastructure should be periodically updated with the latest anti-malware signatures, the bidder shall submit the periodic report on the same with bank.	For an OEM-managed hosted security service, infrastructure anti-malware/endpoint controls are centrally managed and independently audited. We request the Bank to accept OEM security assurance and vulnerability/malware-control attestations rather than periodic host-level signature reports. " The OEM shall maintain appropriate malware protection, vulnerability management, patching and security monitoring controls for the hosted infrastructure. Compliance may be evidenced through independent assurance reports/certifications and applicable security-control attestations instead of customer-specific anti-malware signature update reports."	Please refer addendum for revised clause
2485	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	53	Data Loss Governance and risk management framework shall be defined by bidder for workload on the cloud and same shall be shared with bank on periodic basis. Data loss prevention controls should be implemented to secure the data in the cloud environment from unauthorized or inadvertent exfiltration.	We request clarification that the requirement is intended to ensure protection against unauthorized/inadvertent data exfiltration through the proposed service and appropriate security controls for hosted customer data, rather than requiring disclosure of the OEM's internal cloud governance framework. " The proposed solution shall provide configurable controls to identify and prevent unauthorized or inadvertent transmission/exfiltration of sensitive information through any channels. The OEM shall maintain appropriate access control, encryption and data-protection controls for customer data processed within the hosted service and provide applicable assurance documentation on request."	Please refer addendum for revised clause
2486	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	81	Log generation, storage and review process should be certified by CERT IN empaneled auditor, report for the same shall be submitted by bidder as and when required by bank.	For global SaaS/POD services, security logging and monitoring controls are typically independently audited under recognized assurance frameworks. We request the Bank to accept SOC 2 Type II/ISO 27001 or equivalent independent assurance in lieu of a mandatory CERT-In-empanelled audit of the OEM's internal log-generation/storage/review process. " The OEM shall maintain documented security logging, monitoring, retention and review controls. Effectiveness shall be evidenced through applicable independent third-party assurance reports/certifications such as SOC 2 Type II, ISO 27001 or equivalent. CERT-In-empanelled audit may be required only for bidder-managed components deployed specifically within the Bank environment, where applicable."	Please refer addendum for the revised clause
2487	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	82.5	IT Act 2000 & its amendments, and other Acts/Regulatory guidelines.	Kindly clarify that the OEM must comply with legal/regulatory requirements applicable to it as the provider of the proposed hosted service and provide reasonable documentation to support the Bank's compliance obligations. " OEM shall comply with applicable legal and regulatory obligations relevant to its provision of the proposed service and shall provide available security/privacy/compliance documentation reasonably required to support the Bank's applicable obligations."	Please refer addendum for the revised clause
2488	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	83	CERT IN Empaneled auditor report's is required for the following:	We request the Bank to permit internationally recognized independent assurance reports/certifications for OEM-managed hosted services. CERT-In empanelled audit reports may remain applicable to India-specific bidder-managed/on-premises components where such audit is feasible and required. " For OEM-managed hosted/SaaS services, independent assurance reports/certifications such as SOC 2 Type II, ISO 27001 or equivalent shall be accepted. CERT-In empanelled audit reports shall be applicable only to components/services for which such India-specific audit is contractually and technically feasible."	Please refer addendum for the revised clause
2489	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	92	The application and DB is/will be hosted separately on a dedicated infrastructure (physical/logical) for PSB. Evidence of dedicated infrastructure (physical/logical) for PSB should be submitted.	The proposed platform is an OEM-managed hosted security service designed with logical access controls and customer data isolation. Requiring dedicated physical application/database infrastructure would restrict standard SaaS/POD architectures without necessarily improving the security outcome. We request acceptance of secure logical tenant/customer isolation supported by independent assurance evidence. " The proposed hosted service shall provide secure logical segregation/isolation of Bank data and administrative access from other customers through appropriate access-control and tenant-isolation mechanisms. Dedicated physical application/database infrastructure shall not be mandatory where equivalent logical isolation is implemented and independently assured."	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2490	8	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	98.1	Feasibility to audit/review IT controls of the third party or obtaining independent review report for the same from CERT-In empaneled security consultant, to ensure it meets Bank's information security requirement.	We request that the Bank permit review of current independent assurance reports/certifications as the primary mechanism for reviewing OEM IT controls. Any direct audit should remain subject to the OEM's standard contractual audit provisions, confidentiality, security, scope and advance-notice requirements." The Bank may review applicable independent third-party assurance reports/certifications covering the hosted service. Where additional audit is required, such audit shall be subject to mutually agreed scope, confidentiality/security restrictions, reasonable advance notice and the OEM's standard contractual audit provisions. A CERT-In empanelled consultant may review evidence made available under these conditions."	Please refer addendum for the revised clause
2491	30, 34	7.2.1 Deployment Model & HA (TIP) / 7.2.4.1 Deployment Pattern	Table 7.2.1 Sr. 7; Cl. 7.2.4.1(e)	"Threat Intelligence Platform (TIP) - Cloud (SaaS) + Hybrid - Bank Location: Broker/Collector/Integrator: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR" (Table 7.2.1).	Cyble's Threat Intelligence Platform (TIP) is delivered as a fully cloud-native SaaS solution, providing continuous threat-intelligence aggregation, enrichment and distribution to the Bank via API, STIX/TAXII feed and a dedicated web portal, with high availability, geographic resiliency and disaster recovery built into the SaaS platform itself - fully aligned with the SLA, RTO and RPO defined in Section 13. As the TIP's core function requires no packet-level or in-line processing within the Bank's network, Cyble can meet the Bank's continuity requirement for this solution without deploying a broker/collector component on Bank premises. We request the Bank's confirmation that this cloud-native delivery model will be accepted as fully compliant with Table 7.2.1.	Please refer addendum for the revised deployment requirement
2492	55-56	7.4.3 Attack Surface Management	Cl. 7.4.3	"Discovery of internet-facing and internal assets... The proposed solution shall provide AI-enabled Attack Surface Management (ASM) capabilities for continuous discovery... of the organization's external attack surface, including known and unknown internet-facing assets."	Cyble's Attack Surface Management (ASM) capability provides continuous, AI-enabled discovery, monitoring and risk-prioritization of the Bank's entire external attack surface - internet-facing assets, exposed services, domains, cloud assets and shadow IT - using external/passive reconnaissance together with Bank-shared asset inventories (IP ranges, domains, cloud accounts), with no agent or appliance required inside the Bank's network, consistent with the offsite Managed Service model in Section 7.2.2. This gives the Bank a complete outside-in exposure view from Day 1. We request the Bank's confirmation that this externally-led, agentless approach satisfies Cl. 7.4.3.	Bank is looking for external attack surface management
2493	57	7.4.6 Dark Web Monitoring	Cl. 7.4.6	"...offsite, tool-based continuous dark web and cyber threat exposure monitoring services... across the surface web, deep web, dark web, underground forums, messaging platforms, and data leak repositories."	Cyble's Dark Web & Cybercrime Monitoring capability continuously covers the surface web, deep web, dark web, underground forums, messaging platforms and data-leak repositories, and can begin protecting the Bank's specified identities, brand keywords and domains immediately upon contract signature. To tailor this coverage precisely, we request the Bank share the initial monitoring scope (employee/executive identities, brand keywords, domains and relevant data categories) so Cyble can confirm sizing and reporting cadence.	Details shall be shared with succesful bidder
2494	57	7.4.7 Threat Intelligence Feed	Cl. 7.4.7(l)	"Provision of threat intelligence through a centralized portal/dashboard and/or machine-readable feeds."	Cyble's Threat Intelligence Feed is delivered through both a centralized portal/dashboard and machine-readable, standards-based feeds (STIX/TAXII, MISP-compatible formats and API), enabling seamless integration with the Bank's existing or future security stack whenever required. We confirm this dual delivery model - portal-based consumption plus machine-readable feed/API - and request the Bank's confirmation that it satisfies Cl. 7.4.7.	No Change, Please be guided by the RFP
2495	57-58	7.4.8 Threat Hunting Services	Cl. 7.4.8(m)	"The threat hunting service shall be delivered remotely/offsite using secure and mutually agreed mechanisms for accessing relevant logs, telemetry, security tools, and data made available by the Bank."	Cyble can deliver proactive, intelligence-driven Threat Hunting entirely offsite - correlating curated external threat intelligence (IOCs, IOAs, TTPs, threat-actor and campaign intelligence) against Bank-shared context, supplemented by secure, mutually agreed read-only access to relevant Bank telemetry for validation and deeper investigation as needed - fully consistent with the remote/offsite delivery model mandated in Cl. 7.4.8(m). We request the Bank's confirmation that this intelligence-led hunting model, combined with agreed read-only telemetry access, meets the Bank's requirement.	No Change, Please be guided by the RFP
2496	58	7.4.9 Brand Protection and Monitoring	Cl. 7.4.9(j)	"Takedown coordination with relevant registrars, hosting providers, platforms, application stores, social media platforms, and other relevant entities, wherever applicable."	Cyble's Brand Reputation Monitoring capability continuously identifies brand impersonation, typosquatting, phishing/fraudulent websites, fraudulent mobile apps and social-media impersonation, and actively coordinates takedown requests with registrars, hosting providers, app stores and social platforms on the Bank's behalf under a standard authorisation executed at contract signature - delivering a fully managed, end-to-end takedown process with minimal effort required from the Bank's team. We request the Bank's confirmation that this bidder-led takedown coordination model satisfies Cl. 7.4.9(j).	Please refer addendum for revised clause
2497	256	16.21 Annexure 21: Sizing/Volumetrics (gap for Offsite Services)	Annexure 21, Sizing table	Annexure 21's sizing table provides explicit volumetrics (EPS, endpoint counts, IPs, VPCs, etc.) for the 14 solutions under Section 7.3, but no equivalent executive/VIP count is specified for the offsite services that monitor executive exposure (Anti-Phishing - Cl. 7.4.5, Dark Web Monitoring - Cl. 7.4.6, Brand Protection - Cl. 7.4.9).	Cyble's Executive Monitoring and Digital Risk Protection capabilities can protect any number of the Bank's executives/VIPs from Day 1, with coverage scaled precisely to the Bank's requirement across Anti-Phishing, Dark Web Monitoring and Brand Protection. To finalise sizing, we request the Bank confirm the number of executives/VIPs (e.g., Board members, CXOs, senior management) to be brought under continuous monitoring at contract commencement.	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2498	54	7.4 Functional Requirement - Services (Offsite Services)	Cl. 7.4(d)	"The Bidder shall implement appropriate security controls, including data masking or tokenization for sensitive data, Role-Based Access Control (RBAC), Just-in-Time (JIT) privileged access, and comprehensive audit logging for all services delivered under this RFP." - no named-user/license count is specified for platform/dashboard access to the 9 offsite services.	Cyble's platform can be provisioned for any number of the Bank's analysts, CISO-office and compliance stakeholders who need dashboard access to the offsite services, with full role-based access control as required under Cl. 7.4(d). To size the commercial bid precisely, we request the Bank confirm the number of named analyst/console user licenses required for the Bank's teams to access Cyble's platform and reporting for the proposed offsite services.	details shall be shared with successful bidder
2499	35 of 122	XDR	4.13	The goal is to minimize the attack surface by continuously monitoring, updating, and provide compensatory controls for vulnerabilities and exploits in the endpoints	We request to modify this clause as below "The goal is to minimize the attack surface by continuously monitoring, updating, and provide visibility for vulnerabilities and exploits in the endpoints" Justification: The term "visibility" is outcome-focused and technology-agnostic, allowing solutions to detect and report vulnerabilities through various mechanisms (signatures, behavioral analysis, real-time scanning, etc.), whereas "compensatory controls" is overly prescriptive and implies specific mitigation techniques that may not be applicable to all vulnerability types or endpoint environments. Changing to "visibility" maintains the security intent while enabling bidders to propose diverse, fit-for-purpose solutions without unnecessary implementation constraints.	No Change, Please be guided by the RFP
2500	35 of 122		12	The proposed solution must provide protection against malicious AI application tampering on the endpoints	We request to modify this clause as below "The proposed solution must provide protection against malicious applications tampering on the endpoints" Justification:The "AI" qualifier is overly specific and may exclude non-AI malware threats, creating coverage gaps. The broader term "malicious application tampering" aligns with industry-standard endpoint protection language and ensures comprehensive threat protection regardless of the attack vector or technology employed.	No Change, Please be guided by the RFP
2501	36 of 122		15	The proposed XDR solution must provide comprehensive activity data management and search capabilities, including receiving activity data in the form of telemetry, and metadata; feature for automatic query runs and email notifications; threat matching features using Boolean Logic and other criteria; and options to export, import, delete, and share saved search queries.	We request to modify this clause as below: The proposed XDR solution must provide comprehensive activity data management and search capabilities, including receiving activity data in the form of telemetry, and metadata; feature for automatic query runs and email notifications; threat matching features using Boolean Logic and other criteria; and options to export, delete, and share saved search queries. Justification:The "import" functionality is not a core operational requirement for XDR activity data management. The primary requirements are exporting queries for backup/sharing, deleting obsolete queries, and sharing queries among team members—all of which are standard XDR capabilities. Import functionality introduces unnecessary complexity, potential security/governance risks from external query sources, and is not universally supported across commercial XDR solutions, thereby limiting vendor options unnecessarily	No Change, Please be guided by the RFP
2502	36 of 122		22	The solution should offer options to leverage anti-malware and anti-spyware components stored locally on agents, or signatures stored in-the-vendor cloud	From the operational context and use cases for each deployment option, ensuring continuity of threat protection in all connectivity scenarios. By explicitly defining "when offline" (local components) and "when online" (cloud signatures), the clause removes ambiguity regarding the solution's capability to maintain protective coverage during network disconnections while leveraging updated threat intelligence when connectivity is available We request to modify this clause as below "The solution should offer options to leverage anti-malware and anti-spyware components stored locally on agents when offline, or signatures stored in-the-vendor cloud when online."	No Change, Please be guided by the RFP
2503	36 of 122		29	The solution Device Control capability must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The solution Device Control capability must support Network Devices, USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, time based device control capabilities allowing admin to define the policy specifically for the endpoint operating systems (Windows 10, 11 or higher).	We request to modify the clause as below: The solution Device Control capability must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The solution Device Control capability must support USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, allowing admin to define the policy specifically for the endpoint operating systems (Windows 10, 11 or higher)to allow the devices as required. Justification: Network Devices are typically managed through enterprise network security controls and firewalls rather than endpoint Device Control, and time-based controls create unnecessary operational complexity and maintenance overhead. The modified clause focuses on high-risk local device vectors (USB, Mobile Storage, Bluetooth, Modems) that pose direct security threats to endpoints, while allowing flexibility for organizations to enable specific devices based on business requirements.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2504	37 of 122		43	The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature or through seamless integration with a third-party sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data	We request to amend this clause as below: The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data. Justification: To ensure operational independence and reduce implementation complexity, the organization requires native sandbox functionality built into the core solution rather than relying on third-party integrations, which introduce external dependencies, potential single points of failure, and increase support overhead. This modification mandates that bidders deliver complete sandboxing capability as an integrated component from day 1, ensuring seamless functionality, consistent vendor accountability, and simplified maintenance and support operations without external vendor coordination.	Please refer addendum for revised Clause
2505	38 of 122		57	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	We request to amend this clause as below: The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture or 99.9% availability SLA distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead. Justification: The modification provides architectural flexibility while maintaining the Bank's core availability objective. Not all qualified SaaS vendors employ Active-Active multi-AZ architecture; however, industry-standard 99.9% SLA meets enterprise-grade requirements and enables broader vendor participation without compromising operational resilience. This alternative approach is vendor-agnostic, measurable, and backed by contractual guarantees rather than architectural prescriptions.	Please refer Addendum for revised clause
2506	37 of 122		42	The proposed solution should provide recommended actions to address and mitigate threats detected on endpoints. These remediation suggestions should be informed by forensic data collected from endpoints and detailed analysis performed by the solution to enhance threat response and resolution.	To ensure accurate cost proposals and licensing calculations, please clarify the estimated forensics data volume requirements: a) What is the expected monthly forensics data volume (in GB) that the solution must support? b) What is the planned retention period for forensics data? c) Does this volume include forensics data from all sources (endpoints, servers, cloud workloads, network) or specific sources only? This clarification will enable all bidders to calculate appropriate licensing models and provide consistent cost estimates	Details shall be shared with the successful bidder
2507	54 of 122	Cloud Security	4	The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud envirionment like AWS/Azure/GCP/Meghdoot, AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.	We request to modify this clause as below The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud envirionment like AWS/Azure/GCP/ AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports. Justification: Meghdoot is a comprehensive open-source cloud suite, but bringing it up to PSB requirements demands significant development and integration effort. To be effective, the target cloud environment must be seamless, eliminating the overhead of custom modifications.	Please refer addenudm for revised clause The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud envirionment like AWS/Azure/GCP, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.
2508	Addition of Point as recommendation	Cloud Security	To be Added in Cloud Security	The proposed solution should also support the File scanning with no limitation on file/object type or size covering application across organisation. This should include but is not limited to Amazon Simple Storage Service (S3), Amazon FSx amd Amanzon Elastic File System.	Benefit to PSB: Comprehensive file scanning eliminates critical security blind spots across the organization's cloud storage infrastructure, ensuring no malware, ransomware, or sensitive data can be inadvertently stored in S3, FSx, or EFS without detection. By removing file type and size limitations, the solution prevents attackers from bypassing scanning through obfuscation or leveraging uncommon formats, while the multi-storage coverage consolidates security posture across diverse AWS storage services under a single unified policy. This provides unified threat visibility, enables regulatory compliance (HIPAA, PCI-DSS, GDPR), prevents data exfiltration, and protects against insider threats and supply chain compromises affecting cloud-stored data—significantly reducing the risk of ransomware attacks, compliance violations, and unauthorized data exposure.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2509	page 30 of 273	Extended Detection & Response (XDR)	5	Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Cloud (SaaS): HA Deployment aligned with the SLA, RTO & RPO (Refer Section 13). Management Console: Deployed at both Primary and Secondary sites	We request to amend this clause as below: Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Cloud (SaaS): HA Deployment aligned with the SLA, RTO & RPO (Refer Section 13). Justification: In Appendix 1A clause 27 under XDR explicitly mention for SaaS "ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead" Though it's a SaaS based the management console cannot be deployed at both primary and secondary sites.	Please refer addendum for revised clause
2510	page 31 of 273	Cloud Workload Protection Platform (CWPP)	13	Cloud (SaaS): Deployment aligned with the SLA, RTO & RPO (Refer Section 13).. Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Management Console: Deployed at both Primary and Secondary sites	We request to amend this clause as below: Cloud (SaaS): Deployment aligned with the SLA, RTO & RPO (Refer Section 13).. Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Justification: For SaaS solution the management console cannot be deployed at banks primary & secondary site	Please refer addendum for revised clause
2511	Page 38 of 122 & Page 38 of 122	XDR	22 to 35	These points are duplicate need to be removed	These points are duplicate need to be removed	No Change, Please be guided by the RFP
2512	29, 35 & 259	Sections 7.2.1, 7.2.4.1(b) & 16.21.2	Section 7.2.1 (Deception Technology): "Any agent/Enforcer/Deceptor Standalone at DC and HA, N+N, Standalone at DR." Section 7.2.4.1(b): "The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active	Deception deployment and high-availability topology	The RFP describes the Bank-side deception components as standalone in Section 7.2.1, point no.- 4, but it is also mentioned HA and N+N. We request the bank to kindly clarify that in case we're deploying the solution on-prem, whether Bank needs the solution in Standalone mode/HA mode/N+N mode. Section 16.21.2 (Decoy), point no.-8, Bank has asked that all the inline components of solution should be in HA mode with automatic failover capability. However, the deception solution is not inline. Hence, we request Bank to clarify if they need the Deception Solution in HA. We request the Bank to add on-prem solution also in addition to Cloud/SAAS+Hybrid.	Please refer addendum for revised clause
2513	45, 261 & 262	Sections 7.3.6.2(2) & 16.21.3 - Deployment and Data Retention	Section 7.3.6.2(2): "Restore the logs/data from backup for forensic investigation and as per bank requirement without any additional cost." Section 16.21.3: "Duration of the Contract (Monthly Full backup) - Long-Term Storage (LTS) - Entire Duration of the Contract." The RFP further states that applicable Monthly Full Backups shall be	Backup, restoration and log-retention requirements	We request bank to kindly confirm that if the bank will provide the storage for backup.	No Change, Please be guided by the RFP. Bidder to right size and provide all the required infrastrcuture as per RFP
2514	68	Section 7.7 - On-cloud proposed solution OEM Responsibilities, Point 10	"The OEM shall have valid ISO/IEC 27001 certification and SOC 2 Type II report."	Cloud OEM certification requirement	We request the bank to accept ISO/IEC 27001 or SOC 2 Type II or both.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2515	29, 32 & 35	Sections 7.2.1, 7.2.3 and 7.2.4.1(b)	Section 7.2.1 (Deception Technology): "Cloud (SaaS) + Hybrid" Section 7.2.3: "The solution shall be hosted through a Cloud Service Provider (CSP), either fully as a SaaS service or through a combination of CSP-hosted and Bank-hosted components." Section 7.2.4.1(b): "Deception Technology: The core Deception platform shall be deployed in the	Responsibility for providing the Cloud/SaaS environment	7.2.4.1(b) We request the bank to kindly add the on-prem implementation option also for the core component of the Deception Solution.	Please refer addendum for revised clause
2516	35 & 91	Sections 7.2.4.1(b) and 7.18.1 - Compute Infrastructure, Point 1	Section 7.2.4.1(b): "Deception Technology: The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active configuration. The Cloud/SaaS deployment shall be aligned with the applicable SLA, RTO and RPO requirements."	Hardware and VM infrastructure for Bank-hosted deception components	We request the bank to kindly add the on-prem implementation option also for the core component of the Deception Solution.	Please refer addendum for revised clause
2517	84	Breach and Attack Simulation (BAS)	Sl. No. 1 - Technical Specification	The solution should simulate Ransomware Attacks	Rationale for change: The clause as drafted is a single unqualified statement that every bidder in this category will mark compliant, so it cannot differentiate responses against the 10 marks allotted. It also does not define what constitutes a ransomware simulation. A ransomware validation exercise is only meaningful to the Bank if the platform reproduces the tradecraft ransomware operators actually use, including vulnerable driver loading to terminate endpoint protection, and does so without causing damage on production assets. The Bank is requested to replace the clause with testable criteria covering safe execution of destructive behaviours, deterministic cleanup, and kernel-level attack testing. Proposed modified clause: The proposed solution must execute structurally authentic attacks with destructive elements neutralised, and must be able to trigger destructive-technique detections without the harmful action (for example, testing volume shadow copy deletion detection without deleting the volume shadow copy). It must provide deterministic cleanup mechanisms, safe for execution on production assets, including backup, restore, and removal of all artifacts across: a. File b. Registry c. Service	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2518	84	Breach and Attack Simulation (BAS)	Sl. No. 3 - Technical Specification	The ability to simulate infiltration techniques for breaching a network or infecting a host	Rationale for change: "Infiltration techniques" is undefined and cannot be evaluated objectively. Initial access is the stage at which the Bank's email gateway, secure web gateway and web application firewall are tested, and current adversary tradecraft delivers initial access through container formats such as ISO, IMG, MSI, LNK and ZIP, followed by execution that avoids system interpreters in order to bypass AMSI, script block logging and constrained language mode. A clause that names these delivery and execution requirements allows the Bank to compare bidders on demonstrable capability rather than on a general claim. Proposed modified clause: The proposed solution must dynamically generate container-format payloads including ISO, IMG, MSI, LNK, and ZIP variants containing executables, shortcuts, or DLL hijack chains, and deliver them via uniquely generated URLs per simulation to comprehensively validate email gateway, secure web gateway, and WAF filtering against modern initial-access techniques such as ISO-LNK-DLL chains. The simulation agent must execute malicious behaviours and adversary techniques without reliance on system interpreters including PowerShell, CMD, BASH, or SH, validating control effectiveness against modern adversary tradecraft that increasingly avoids interpreter-based execution to bypass AMSI,	No Change, Please be guided by the RFP
2519	84	Breach and Attack Simulation (BAS)	Sl. No. 6 - Technical Specification	The solutions should test Security Operations Center (SOC) detection capability of bank by simulating multi-chained payloads with advanced evasion methods including DLL Hijacking, Process Injection, and PPID spoofing for breaching and infiltrating the network.	Rationale for change: The clause names only three evasion techniques and does not state that they must be executed as real behaviours on the asset rather than logged as simulated steps. SOC detection validation succeeds or fails on two things the clause does not capture: whether the payload natively performs modern evasion against the deployed control stack, and whether each technique is available in multiple procedure variants, since a detection that catches one implementation of LSASS credential dumping routinely misses six others. The Bank is requested to expand the clause so that detection coverage is validated across the attacker variant space. Proposed modified clause: The simulation payload execution must natively perform the following techniques as executed behaviours against the deployed control stack: a. EDR unhooking (NTDLL unhooking, direct and indirect syscalls) b. Reflective DLL injection c. Process hollowing d. PPID spoofing e. Command-line argument spoofing f. Fileless in-memory execution For each in-scope MITRE ATT&CK technique, the proposed	No Change, Please be guided by the RFP
2520	84	Breach and Attack Simulation (BAS)	Sl. No. 7 - Technical Specification	The solution should have the ability to create custom use cases / simulations attacks according to bank's requirement.	Rationale for change: As drafted the clause is satisfied by a script upload field or by a vendor professional services engagement, both of which leave the Bank dependent on the OEM for every new scenario and carry recurring cost. For the Bank's own security team to build scenarios for proprietary applications and internal workflows, the clause should require a user interface driven attack creator with named configurable parameters. Proposed modified clause: The proposed solution must provide a UI-driven attack creator enabling customer security teams to design custom multi-stage simulations with configurable name, description, MITRE category, execution privileges (User/Admin), payload type (DLL/EXE/Service/ISO/MSI/LNK), and chained secondary behaviours supporting organisation-specific scenario testing for proprietary applications, internal workflows, and bespoke attack hypotheses.	No Change, Please be guided by the RFP
2521	84	Breach and Attack Simulation (BAS)	Sl. No. 8 - Technical Specification	The solution must allow the execution of simulations on multiple agents simulataneously. An attack chain must be executed on multiple endpoints agents at the same time to provide unique attack specific insights across the deployed agents in the organisation.	Rationale for change: The clause states the requirement for simultaneous execution but does not exclude sequential execution presented as a single campaign, which is how several solutions in this category operate. It also does not address the operational prerequisites for running simulations across a bank-scale estate: the agent must be deployable at scale through Group Policy or golden image, must run silently so that branch and business users are not alerted or disrupted, and must update centrally without re-imaging or desk visits. The Bank is requested to make both the concurrency model and the deployment model explicit. Proposed modified clause: The proposed solution must execute a single coordinated attack campaign across multiple agents, business units, and geographies simultaneously, not sequentially (i.e. One Kill chain, run on multiple Endpoint Targets at the same time), producing independent per-agent evidence consolidated into a unified campaign report. Solutions that walk through agents one-by-one cannot realistically validate enterprise-scale concurrent compromise scenarios. The simulation agent must be a lightweight software package suitable for enterprise mass-deployment via Group Policy Object (GPO), golden image baking, or standard endpoint management tooling, requiring no per-host configuration post-installation.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2522	84	Breach and Attack Simulation (BAS)	Sl. No. 11 - Technical Specification	The solution should support technical integrations with bank's existing solutions (e.g., SIEMs, ticketing systems, log management, Firewalls, automation/orchestration, analytics solutions, threat intelligence solutions, etc.)	Rationale for change: "Should support technical integrations" is unverifiable and is routinely answered with roadmap commitments or bespoke development quoted after award. For closed-loop validation, where a simulation result is correlated against the alert raised in the Bank's SIEM and a ticket is created automatically, the Bank needs a documented API, automation tooling and pre-built connectors available at the time of bid. The Bank is requested to make the integration requirement specific and verifiable. Proposed modified clause: The proposed solution must expose a RESTful API with publicly available OpenAPI documentation, provide an open-source CLI and SDK for automation, and ship pre-built integrations with major SIEM, SOAR, ITSM, EDR, firewall, and email gateway vendors to enable closed-loop validation of alerts, automated ticket creation, and detection correlation.	No Change, Please be guided by the RFP
2523	30	RFP - 7.2 Solution & Services Deployment Model and Their HA Requirement 7.2.1 Solutions – Master Deployment Matrix	6. Network Detection & Response (NDR)	Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Management Console: Deployed at both DC and DR	Different NDR solution works on different redundancy deployment methodology (I.e Active - Active or Active - Passive). Request bank to modify the clause as: Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active/Passive at DC and HA, N+N, Active-Active/Passive at DR. Management Console: Deployed at both DC and DR	Please refer addendum for revised clause
2524	45	RFP - Scope of Work 7.3.5 Network detection and response (NDR)	7.3.5.1 Modules, Architecture & Deployment:	Pt 2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Generally NDR solutions are deployed with sole purpose of doing network analysis, threat detection & response and does not have native 2FA capability, so request bank to remove this point. As an alternate as proposed in same point, proposed NDR solution can be integrated with bank's existing MFA solution.	Please refer addendum for the revised clause
2525	49	RFP - Scope of Work 7.3.10 Application security testing Tool	7.3.10.1 Modules, Architecture & Deployment:	Pt 2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Generally AST solutions are deployed with sole purpose of scanning the source code, web, api etc and does not have native 2FA capability, so request bank to remove this point. As an alternate as proposed in same point, proposed AST solution can be integrated with bank's existing MFA solution.	No Change, Please be guided by the RFP
2526	110	RFP - 10.2 Eligibility Evaluation Criteria	OEM Evaluation Criteria	Pt 19. The proposed OEM SIEM Solution with a minimum capacity of 30,000 EPS or 1.2 TB/day shall have been successfully implemented on cloud in one (1) in India.	For wider participation, we request bank to amend the clause as: The proposed OEM SIEM Solution with a minimum capacity of 5,000 EPS or.2 TB/day shall have been successfully implemented on cloud in any one (1) Govt/PSU customer in India. OR The proposed OEM SIEM Solution with a minimum capacity of 10,000 EPS or.4 TB/day shall have been successfully implemented on cloud in one (1) in India.	Please refer addendum for revised clause.
2527	112	RFP - 10.2 Eligibility Evaluation Criteria	OEM Evaluation Criteria	Pt 20. The proposed OEM solution should have been implemented in at least one BFSI is to be submitted for the following solutions: NDR	For wider participation, we request bank to amend the clause as: The proposed OEM solution should have been implemented in at least one BFSI / Govt is to be submitted for the following solutions: NDR	Please refer addendum for the revised clause
2528	260	RFP - 16.21.2 Volumetrics- Solution-wise Requirements	12. Application Security Testing Tool	All the inline components of the solution must operate in high availability mode. In the event of any component failure, the system should automatically initiate failovers within seconds, ensuring uninterrupted functionality without requiring manual intervention.	Application Security Testing as a technology in general works at developemnt/pre-production/UAT stage only. And hence as a solution there is no need of high availability mode. Same has already been updated in this RFP (as solution is asked in standalone at both DC & DR). So, request bank to deleted this clause.	No Change, Please be guided by the RFP. The bidder must design the solution to fully comply with the RFP requirements, ensuring that in case of a failover, the system meets the defined SLA for availability, RTO, and RPO. The bidder is required to adhere to the deployment requirements outlined in the RFP when designing and proposing the solution architecture.
2529	40	APPENDIX 1A Functional Compliance Sheet (Solutions)	Network Detection & Response (NDR)	Pt 8. Proposed solution should generate a root cause analysis, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets.It should provide a platform for easier investigation like visual graphical view and timeline of the attack and it should support tagging of MITRE tactics, techniques and procedures used by the attacker in alerts and incidents.	We reqeust bank to amend the clause: Proposed solution should generate a root cause analysis / incident management, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets.It should provide a platform for easier investigation like visual graphical view and timeline of the attack and it should support tagging of MITRE tactics, techniques and procedures used by the attacker in alerts and incidents.	Please refer addendum for the revised clause
2530	40	APPENDIX 1A Functional Compliance Sheet (Solutions)	Network Detection & Response (NDR)	Pt 13. The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	As bank has asked for on-premise solution for NDR, on the contrary, this clause asks for cloud-native SAAS ask. So, we kindly request bank to delete this clause.	Please refer Addendum for revised clause
2531	42	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 3. The solution must be able to analyse a wide array of programming languages including Java,.Net, C/C++, Objective-C, Android, PHP, COBOL, Ruby, Swift, HTML 5, Scala, APEX, TypeScript, Go, Kotlin and ABAP etc but not limited to these alone	Considering the future requirements of AI in Secure Code Development and most of the development is moving towards AI generated code using AI supported languages. So it is very important for bank to have coverage around this as well and will recommend to incorporate AI supported languages like "R, Ada, Solidity, Bash, Groovy, Rust, Perl", but not limited to these alone.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2532	42	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 24. Solution should support Machine learning and Analysis based on the archived results	ML capability is important, but it is very important to have coverage around AI based code as well. And will recommend bank to consider: The solution should have the capability to scan AI generated code. The solution should be able to integrate with AI coding agent via MCP	No Change, Please be guided by the RFP
2533	43	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 32. The solution should be able to support Composition Analysis: Identify the opens source components used in the application. Vulnerabilities & outdated version Licensing risk associated with the components	Bank is looking for Software composition analysis and asked for identifying the open source component and licensing risk. But this limited information is not enough for bank to secure themselves with rapidly increasing supply chain attacks and we will highly recommend to consider following as well: SCA system must catalogue open source components from Maven, NPM, and Nuget. SCA system has to be able to generate a Bill of Materials for an application. Solution should have the ability to continuously monitor the scanned components & notify if there are any zero day attacks without performing the rescan. Solution should Catalog, Store, and Audit SBOMs (both cycloneDx & SPDX) generated for in-house developed software applications and COTS applications.	No Change, Please be guided by the RFP
2534	30	7.2 Solution & Services Deployment Model and Their HA Requirement 7.2.1 Solutions – Master Deployment Matrix	Sl. No. 8	Vulnerability assessment (VA) & vulnerability lifecycle management Bank Location: Standalone at DC and Standalone at DR. Management Console: Deployed at both DC and DR	Requesting clarifications if standalone management console in DR will be live or will be on standby ?	Please refer addendum for revised clause
2535	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 1 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall be deployable entirely on-premises and shall not require any cloud-hosted component, external service, or Internet connectivity for its core functionality, scanning, management, reporting, analytics, or product capabilities.	Requesting change to: The proposed solution shall be deployable entirely on-premises or hosted on MeitY cloud or Meity empanelled cloud environment. No data shall be shared with the platform/cloud outside India geolocation.	Please refer addendum for the revised clause
2536	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 3 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall be software-based and fully deployable on the hardware infrastructure proposed by the Bidder.	Requesting change to: The proposed solution shall be software-based and fully deployable on the hardware infrastructure or should support hybrid- on-premise architecture with management-console or scanners on on-premise and analytics components on MeitY/MeitY-emapanneled cloud proposed by the Bidder.	No Change, Please be guided by the RFP
2537	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 9 of Vulnerability Assessment & vulnerability lifecycle Management	Each scanning engine shall support web application security assessment together with traditional infrastructure vulnerability and configuration/compliance assessment. The solution shall identify vulnerabilities, missing patches, insecure configurations, and compliance deviations, and generate comprehensive reports containing risk severity, evidence of findings, affected assets, and remediation recommendations to support security governance, audit, and regulatory compliance.	Requesting to confirm that if DAST specs are specifically provided for web-application's VAPT, then what is the scope of "web-application" scanning in this spec? Also requesting to share the total number of web-applications considered in the scanning scope.	No Change, Please be guided by the RFP
2538	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 18 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall support both active and passive asset discovery and vulnerability assessment/scanning.	Requesting change to: The proposed solution shall support both active and/or passive asset discovery and vulnerability assessment/scanning.	No Change, Please be guided by the RFP
2539	48	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 27 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall support both active and passive techniques for vulnerability detection, where applicable.	Requesting change to: The proposed solution shall support both active and/or passive techniques for vulnerability detection, where applicable.	No Change, Please be guided by the RFP
2540	48	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 33 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall support deployment and lifecycle management of scanning agents without dependency on cloud-hosted services.	Requesting change to: The proposed solution shall support deployment and lifecycle management of scanning agents.	No Change, Please be guided by the RFP
2541	48	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 34 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall assess Active Directory security posture and identify misconfigurations, privilege risks, insecure policies, and exposure of critical directory services.	Requesting to clarify that this spec is already addressed in IDTR then what is the requirement of it in VM solutin?	No Change, Please be guided by the RFP
2542	49	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 74 of Vulnerability Assessment & vulnerability lifecycle Management	The solution shall support offline signature and plugin updates for deployment in isolated or air-gapped environments.	Requesitng to remove this spec because if the cloud-based solution is offered and where cloud is hosted on MeitY cloud or MeitY empanneled cloud then questions related to air-gap environment doesn't arise.	No Change, Please be guided by the RFP
2543	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 81 of Vulnerability Assessment & vulnerability lifecycle Management	The solution shall support password-protected and/or digitally signed reports with configurable retention and archival.	Requesting change to: The solution must support secure, encrypted report distribution (including native PGP encryption) and enforce strict role-based access controls (RBAC) for report viewing. Additionally, the platform must provide configurable cloud-based data retention policies alongside automated options to archive historical scan data and reports to external storage	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2544	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 87 of Vulnerability Assessment & vulnerability lifecycle Management	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	Requesting change to: The solution must provide AI-generated risk summaries and plain-language vulnerability briefs that automatically fuse asset criticality, technical findings, and real-world threat telemetry (such as CISA KEV and EPSS data) to streamline IT triage. If cloud analytics are utilized to run these machine learning models, the solution vendor must guarantee that all data is isolated within dedicated, bank-authorized cloud regions, employing strict data privacy frameworks that ensure source code, credentials, and raw scan parameters are explicitly excluded from public AI training models or multi-tenant public AI services	Please refer addendum for revised clause
2545	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 88 of Vulnerability Assessment & vulnerability lifecycle Management	Unified, correlated findings intelligence. Every scanning engine — across web, API, network and host, cloud, containers, mobile, source code, device configuration and identity — reports into a single normalized findings model..	Requesting clarification on why unified reporting is asked as the ASM, VM, DAST solutions are considered separately.	No Change, Please be guided by the RFP
2546	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 90 of Vulnerability Assessment & vulnerability lifecycle Management	Mobile Application Security Testing: The proposed solution shall support static security analysis of Android and iOS mobile application packages, including APK/AAB and IPA formats, and shall provide security assessment mapped to recognized mobile application security standards and methodologies such as OWASP MASVS and MASTG.	Requesting clarification for the spec as the ask is for DAST or MAST solution.	No Change, Please be guided by the RFP
2547	87	Anti Phishing Services	17.1	Solution should detect at the earliest point in the attack, post initial compromise as the attacker is first attempting to move laterally and escalate privilege.	Since this section is focused on Anti-Phishing, we understand that the objective is to identify suspicious activity following a successful phishing or account-compromise event. Network-level lateral movement and deception capabilities may be addressed by other security controls. We request the Bank to clarify whether this clause may instead focus on early post-compromise user activity visibility for the Bank's most critical users. " The solution should support early identification and investigation of suspicious user activities associated with potential account compromise following phishing or other email-originated attacks, with enhanced user activity monitoring for up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles."	Please refer to the relevant Addendum for updated specfications
2548	87	Anti Phishing Services	17.4	Solution must provide robust supply chain and AI/ML-driven contact chain analysis capabilities to identify and defend against socially engineered, impersonated, or BEC attacks.	As compromise of trusted suppliers and partners is an important source of BEC and phishing risk, we request the Bank to clarify whether the existing supply-chain requirement should explicitly include behavioural analysis of supplier/partner communication patterns to identify attacks originating from compromised trusted accounts. " Solution must provide robust supply-chain and AI/ML-driven contact-chain and behavioural analysis capabilities to identify and defend against socially engineered, impersonated or BEC attacks, including threats originating from compromised or impersonated supplier/partner accounts."	Please refer to the relevant Addendum for updated specfications
2549	87	Anti Phishing Services	18	Solution must proactively analyze suspicious URLs using dynamic/behavioral analysis to prevent the spread of malware and other threats.	The RFP separately addresses URL analysis and post-delivery remediation. We request clarification whether these requirements are intended to provide continuous protection throughout the email threat lifecycle, including pre-delivery analysis, click-time URL protection and post-delivery detection/remediation. " Solution must provide continuous protection across the email threat lifecycle, including pre-delivery threat detection, real-time/click-time inspection of suspicious URLs, and post-delivery detection and automated remediation of threats that are subsequently determined to be malicious."	Please refer to the relevant Addendum for updated specfications
2550	88	Anti Phishing Services	19.7	Solution must be able to offer a comprehensive portal that allows users to access information and metadata on events/incidents, facilitating network threat forensics for thorough investigation and analysis of potential security breaches or incidents.	To strengthen investigation of phishing-led incidents involving executives and other critical users, we request clarification whether the existing forensic portal requirement may also include contextual user and endpoint activity for a limited population of Bank-identified critical/high-risk users. " Solution must offer a comprehensive investigation portal providing information and metadata on events/incidents for forensic analysis. For up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, the portal should additionally provide contextual user and endpoint activity, including relevant application, file and user-action details, to support investigation of potential phishing-led compromise."	Please refer to the relevant Addendum for updated specfications
2551	88	Anti Phishing Services	19.9	Solution must empower security operations and incident responders to automate the identification, remediation, and sharing of phishing threats, streamlining the process of detecting, addressing, and disseminating information about potential phishing attacks for improved response and mitigation.	To improve SOC investigation efficiency, we request clarification whether the existing phishing identification and remediation requirement should include centralized attack context showing why a message was identified as malicious, the users targeted, associated threat indicators and remediation status. " Solution must empower security operations and incident responders to automate identification, investigation, remediation and sharing of phishing threats, and should provide centralized contextual visibility into the users targeted, associated threat indicators, detection rationale, attack characteristics and remediation actions."	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2552	88	Anti Phishing Services	19.1	Solution must provide incident responders with real-time analytics and visibility into email-based attacks targeting the organization.	Email-based attacks against executives and privileged users may require additional context after delivery to determine whether a targeted user has subsequently performed suspicious activity. We request the Bank to clarify whether real-time investigation visibility may include relevant user activity context for up to 100 Bank-identified critical/high-risk users. " Solution must provide incident responders with real-time analytics and visibility into email-based attacks targeting the organization. For up to 100 Bank-identified critical/high-risk users, the solution should additionally provide contextual visibility into suspicious user activities associated with potential phishing or account compromise, including relevant user, endpoint, application and file activity."	Please refer to the relevant Addendum for updated specfications
2553	88	Anti Phishing Services	19.23	Solution must have simplicity of evaluation and additional visibility into internal traffic and other communication channels can reduce risk, and baseline user activity to detect suspicious behavior.	The existing clause already seeks baselining of user activity to detect suspicious behaviour. We request the Bank to clarify the intended depth and scope of this capability and whether enhanced monitoring may be applied to a focused population of up to 100 Bank-identified critical/high-risk users, where deeper visibility provides the greatest security value. " Solution must provide additional visibility into relevant internal activity and communication channels to reduce risk and baseline user activity to detect suspicious behaviour. Enhanced user and data activity monitoring should be provided for up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, with configurable detection policies for suspicious, anomalous or policy-violating activities."	Please refer to the relevant Addendum for updated specfications
2554	90	Anti Phishing Services	19.7	Solution must provide protection against harassment mail and mitigate the risks associated with emails from unknown senders specifically for executives or VIPs, safeguarding them from potential threats and ensuring their email communication remains secure.	Since this clause already provides enhanced protection for executives/VIPs, we request the Bank to clarify whether such enhanced protection should extend beyond receipt of suspicious email to investigation of risky user and data activities that may occur following phishing or account compromise, for a limited set of the Bank's most critical users. "Solution must provide protection against harassment mail and mitigate risks associated with emails from unknown senders specifically for executives or VIPs. For up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, the solution should additionally provide enhanced visibility into risky user and data activities following suspected phishing or account compromise, including relevant file movement, web/upload activity, removable-media activity and other supported data-transfer channels."	Please refer to the relevant Addendum for updated specfications
2555	52	Idendity Threat Detection and Response (ITDR)	1.7	Detect and respond to active threats with high fidelity (low false positives and false negatives).	The Bank has separately specified a comprehensive deception platform for detection of active attacker activity, reconnaissance and lateral movement. We understand that the intent of this clause within ITDR is therefore to complement those controls with focused monitoring of the Bank's most critical identities. Considering that enhanced user-activity monitoring is most relevant for high-risk personnel such as executives, privileged users and other critical users, we request the Bank to kindly clarify whether this requirement may be read as follows: " Identity Threat Detection Solution should provide high-fidelity detection and response for risky or anomalous user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, to identify activities associated with careless, malicious or compromised users. "	No Change, Please be guided by the RFP
2556	52	Idendity Threat Detection and Response (ITDR)	1.8	Provide contextual information—who, what, when and how—to inform all stages of the attack chain.	The Bank has already sought attack-lifecycle visibility under the separate deception requirements. For ITDR, we understand that additional value would be derived from detailed user-centric context for the Bank's most critical identities, enabling investigation of risky activity performed by such users. We request the Bank to kindly clarify whether this requirement may be read as follows: " Identity Threat Detection Solution should provide contextual information—who, what, when, where and how—around risky user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, to support investigation and response."	No Change, Please be guided by the RFP
2557	52	Idendity Threat Detection and Response (ITDR)	1.9	Provide deep insights into both the potential and used privilege escalation and lateral movement steps in an attack.	Privilege escalation and lateral-movement visibility is already substantially addressed under the separately specified deception solution, including attacker lifecycle visibility, MITRE ATT&CK mapping, deceptive attack paths and detection of lateral movement. To avoid duplication while retaining complementary investigation capability for high-risk identities, we request the Bank to kindly clarify whether this requirement may be read as follows: "Identity Threat Detection Solution should provide deep insights into activities performed by up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, covering application usage, file and data movement, endpoint activity and other risky behaviours to support investigation of compromised, malicious or negligent user activity."	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2558	52	Idendity Threat Detection and Response (ITDR)	2.9	Detect all types of attack vectors including pre-attack reconnaissance, zero-day attacks, privilege escalation prevention, lateral movement and data theft.	Pre-attack reconnaissance, lateral movement, malware/attack behaviour and attacker lifecycle visibility are already covered under the Bank's separate deception specifications. We understand that the complementary requirement under ITDR should focus on identity/user risk and potential data-loss activity for the Bank's most critical users rather than duplicate the deception control. We request the Bank to kindly clarify whether this requirement may be read as follows: " Identity Threat Detection Solution should detect risky user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, including suspicious application usage, unauthorized access or movement of sensitive information, removable-media activity, web-based transfer, cloud synchronization and other potential data-exfiltration activities."	The Clause is applicable only to idendity related threat vector only. The volumetrics is provided in the RFP and should be complied
2559	52	Idendity Threat Detection and Response (ITDR)	2.10	Detect multiple attacks simultaneously.	We understand the intent is to ensure that the solution is not restricted to investigation of a single event at a time. Since active attacker detection is separately covered by the deception solution, we request that this clause be clarified in terms of concurrent monitoring and investigation of risky activities across the Bank's designated critical-user population: "Identity Threat Detection Solution should be capable of detecting and investigating multiple risky user and data activities simultaneously across up to 100 critical/high-risk users and their monitored endpoints."	No Change, Please be guided by the RFP
2560	52	Idendity Threat Detection and Response (ITDR)	3.2	Provide unified presentation of both source- and target-based telemetry data in a timeline view.	The Bank has separately specified end-to-end attacker visibility and behavioural analysis under the deception solution. For ITDR investigations involving critical identities, a chronological user-activity view would provide complementary evidence of actions performed by the user. We request the Bank to kindly clarify whether the requirement may be read as follows: " Identity Threat Detection Solution should provide a unified chronological timeline of user- and endpoint-based activity telemetry for up to 100 critical/high-risk users identified by the Bank to support investigation of risky or suspicious user activity."	No Change, Please be guided by the RFP
2561	52	Idendity Threat Detection and Response (ITDR)	3.3	Correlate identity-related telemetry from relevant source and target systems to identify and investigate identity compromise, privilege escalation, credential abuse and lateral movement.	Privilege escalation and lateral-movement detection are already addressed through the separately specified deception controls. To provide complementary investigation capability for the Bank's highest-risk identities, we request the Bank to clarify whether this clause may focus on correlation of user, endpoint, application and data activity for the designated critical-user population: " The solution shall support correlation of user, endpoint, application and data-activity telemetry for up to 100 critical/high-risk users identified by the Bank to identify and investigate suspicious user behaviour, sensitive-data movement, policy violations and potential data-exfiltration activities."	No Change, Please be guided by the RFP
2562	52	Idendity Threat Detection and Response (ITDR)	3.4	Integrate with compatible endpoint/extended detection solution to capture screen recordings or screenshots during active attacker sessions as advanced forensic evidence.	The Bank has separately specified attacker-session and forensic visibility through the deception platform. Within ITDR, we understand that visual evidence is intended to strengthen investigation of high-risk user activity. We request the Bank to kindly clarify whether the requirement may be read in an outcome-based manner for the designated critical-user population: " The Identity Threat Detection Solution should support screenshots, screen capture or equivalent visual evidence of relevant activity for up to 100 critical/high-risk users during suspicious or high-risk user sessions, as part of forensic investigation and evidence collection."	Please refer addendum for revised clause.
2563	52	Idendity Threat Detection and Response (ITDR)	3.5	Integrate with compatible network detection solution to support collection of PCAP data for network-level incident visibility.	The requirement for PCAP is network-centric and does not directly relate to identity posture or focused user-activity monitoring. Further, the Bank's separate deception specifications already require high-interaction decoys, recording of attacker activities, traffic/behaviour visibility, forensic investigation and integration with network/security technologies. To avoid duplication of network-level forensic controls across two solution categories, we request the Bank to kindly delete this clause from the ITDR section.	Please refer addendum for revised clause.
2564	52	Idendity Threat Detection and Response (ITDR)	3.6	Push incident data into SIEM/XDR or SOAR technologies via integrations for improved incident management.	We understand that the objective is to ensure relevant ITDR alerts and investigation context are available to the Bank's SOC ecosystem. For the enhanced monitoring of designated critical users, we request the Bank to kindly clarify whether alerts and activity information may be shared through supported integrations or APIs as follows: " Identity Threat Detection Solution should make alerts and relevant incident/activity data for the monitored critical-user population available to SIEM/XDR, SOAR or other supported security platforms through integrations or APIs for improved incident management."	The proposed solution hould be integrated with SIEM/XDR or SOAR technologies for sharing the incident data via supported integrattion or APIs
2565	52	Idendity Threat Detection and Response (ITDR)	3.7	As part of forensic data collection, include detailed attack path information including protocols leveraged during the attack.	Detailed attack-path and attacker-behaviour visibility is already sought under the separate deception specifications, including deceptive attack paths, MITRE ATT&CK mapping and forensic investigation. To avoid overlap while retaining complementary evidence for investigations involving the Bank's critical identities, we request the Bank to kindly clarify whether the requirement may be read as follows: " Identity Threat Detection Solution should, as part of forensic data collection for up to 100 critical/high-risk users, include detailed user-activity information such as applications used, files accessed, data movement, destination channels and other relevant endpoint activity associated with the incident."	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2566	52	Idendity Threat Detection and Response (ITDR)	3.8	Collect user and computer information from Active Directory as part of forensic data gathering to enhance context and assess risk exposure.	We understand that directory information is required to enrich investigations with user and computer context. We request the Bank to clarify that enterprise identity context may be maintained for the overall identity population, while detailed endpoint/user-activity telemetry may be applied to the Bank's designated critical-user population: " Identity Threat Detection Solution should use relevant user and computer identity information to enhance forensic context and risk assessment, and should correlate such context with detailed endpoint/user-activity telemetry for up to 100 critical/high-risk users identified by the Bank."	Please refer addendum for revised clause
2567	52	Idendity Threat Detection and Response (ITDR)	3.9	Detect an adversary's attempt to move laterally toward key assets using as many Windows, Mac or Linux hosts as possible without requiring a persistent agent.	The Bank's separate deception specifications expressly require detection of lateral movement, reconnaissance, credential theft and malicious activity using agentless and/or agent-based deception techniques across the enterprise. The present clause therefore duplicates a capability already being procured under the Deception section. To avoid overlapping scope and duplicate controls, we request the Bank to kindly delete this clause from the ITDR section.	Please refer addendum for revised clause
2568	52	Idendity Threat Detection and Response (ITDR)	3.10	Collect AD user/computer information for forensic context and detect at the earliest point post initial compromise as the attacker first attempts lateral movement and privilege escalation.	Early detection of lateral movement and privilege-escalation activity is substantially covered under the Bank's separate deception requirements. To retain a complementary identity/user-risk objective without duplicating the deception scope, we request the Bank to kindly clarify whether this clause may focus on early detection of risky activity among the designated critical-user population: " Identity Threat Detection Solution should use relevant identity context and detect risky user behaviour at the earliest possible point for up to 100 critical/high-risk users, based on monitored endpoint activities and configured detection policies, enabling investigation and response before such activity results in significant data loss or business impact."	Please refer addendum for revised clause
2569	52	Idendity Threat Detection and Response (ITDR)	3.11	Collect AD user/computer data during forensic gathering while ensuring all deception techniques remain hidden from legitimate users.	The requirement to ensure deception techniques remain hidden from legitimate users is inherently a deception-platform capability. The Bank has already included comprehensive deception requirements covering lures, breadcrumbs, fake credentials, deceptive assets, attacker engagement and techniques designed to remain undetected by attackers. We therefore request the Bank to kindly delete this clause from the ITDR section to avoid duplication.	Please refer addendum for revised clause.
2570	2	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	10	OEM shall ensure compliance of the complete proposed solution & platform with RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and all applicable regulations throughout the contract period.	We request the Bank to clarify that the OEM is required to maintain applicable security, privacy and regulatory controls relevant to the services provided and furnish available compliance/assurance documentation, while the overall regulatory compliance obligation of the Bank remains subject to the Bank's deployment, configuration and usage of the service. " OEM shall maintain security, privacy and compliance controls applicable to the proposed hosted service and shall provide available independent assurance reports, certifications and relevant compliance documentation to support the Bank's obligations under applicable RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and other applicable regulatory requirements."	Please refer addendum for revised clause
2571	2	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	20	The Service uptime agreement for the proposed solution on cloud should have monthly uptime commitments and have transparent monthly credit calculations in case of uptime not being met for any services.	We understand that published/contracted OEM hosted-service SLA commitments and corresponding service-credit methodology shall meet this requirement. Kindly confirm.	No Change, Please be guided by the RFP
2572	3	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	29	Solution provider should provide the design and process for data deletion in the scope of an independent audit and that the operational effectiveness of these controls is tested. The report for the same should be submitted to bank as and when asked by bank.	For a globally operated hosted security service, control effectiveness is generally evidenced through independent assurance reports such as SOC 2 Type II and documented data-retention/deletion controls. We request the Bank to permit such independent assurance documentation instead of requiring a separate bespoke data-deletion audit report. " Solution provider shall maintain documented secure data-retention and deletion controls. Compliance may be demonstrated through applicable independent third-party assurance reports/certifications (such as SOC 2 Type II or equivalent) and documented data-retention/deletion policies made available subject to OEM confidentiality requirements."	Please refer addendum for the revised clause
2573	4	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	41.3	Independent audit for testing effectiveness of secure data removal, such that data is rendered permanently inaccessible. (Including any backup or distributed online media).	We request the Bank to accept independently audited secure deletion and media-management controls, together with documented retention/deletion periods, rather than requiring a customer-specific audit of all backup and distributed media. " The OEM shall maintain secure data deletion, media handling and backup-retention controls designed to render customer data inaccessible in accordance with documented retention schedules. Effectiveness may be evidenced through independent assurance reports such as SOC 2 Type II/ISO 27001 or equivalent and relevant OEM security/privacy documentation."	Please refer addendum for the revised clause
2574	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	47.2	Bank shall have an option to implement 'Bring Your Own Key' as and when required.	The proposed service protects data at rest and in transit using strong encryption; however, customer-managed infrastructure encryption keys are not a standard capability of the hosted anti phishing service. We request deletion of the BYOK requirement, or acceptance of OEM-managed enterprise-grade encryption and key-management controls. " Requested Action: Delete the BYOK requirement. Alternatively: 'Data processed/stored by the hosted service shall be protected using industry-standard encryption in transit and at rest, with secure OEM-managed key-management controls subject to independent security assurance.'"	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2575	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	49	Web Application Firewall shall be implemented on the cloud for Web based applications. WAF application signature should be updated and reviewed regularly. The Report shall be submitted to bank on a periodic interval.	Since the proposed platform is an OEM-managed hosted security service, underlying WAF technology, signatures and configurations form part of the OEM's internal security architecture and may not be exposed as customer-specific reports. We request the Bank to accept periodic VAPT/penetration-test assurance or equivalent independent security assessment evidence covering the hosted application instead of WAF signature reports. " The hosted web application/platform shall be protected through appropriate application-security controls. The OEM shall conduct periodic vulnerability assessment and penetration testing/security assessments and, subject to confidentiality restrictions, provide an executive summary/attestation or applicable independent assurance evidence to the Bank on request. Customer-specific WAF signature reports shall not be mandatory."	Please refer addendum for revised clause
2576	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	52	The systems in cloud infrastructure should be periodically updated with the latest anti-malware signatures, the bidder shall submit the periodic report on the same with bank.	For an OEM-managed hosted security service, infrastructure anti-malware/endpoint controls are centrally managed and independently audited. We request the Bank to accept OEM security assurance and vulnerability/malware-control attestations rather than periodic host-level signature reports. " The OEM shall maintain appropriate malware protection, vulnerability management, patching and security monitoring controls for the hosted infrastructure. Compliance may be evidenced through independent assurance reports/certifications and applicable security-control attestations instead of customer-specific anti-malware signature update reports."	Please refer addendum for revised clause
2577	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	53	Data Loss Governance and risk management framework shall be defined by bidder for workload on the cloud and same shall be shared with bank on periodic basis. Data loss prevention controls should be implemented to secure the data in the cloud environment from unauthorized or inadvertent exfiltration.	We request clarification that the requirement is intended to ensure protection against unauthorized/inadvertent data exfiltration through the proposed service and appropriate security controls for hosted customer data, rather than requiring disclosure of the OEM's internal cloud governance framework. " The proposed solution shall provide configurable controls to identify and prevent unauthorized or inadvertent transmission/exfiltration of sensitive information through any channels. The OEM shall maintain appropriate access control, encryption and data-protection controls for customer data processed within the hosted service and provide applicable assurance documentation on request."	Please refer addendum for revised clause
2578	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	81	Log generation, storage and review process should be certified by CERT IN empaneled auditor, report for the same shall be submitted by bidder as and when required by bank.	For global SaaS/POD services, security logging and monitoring controls are typically independently audited under recognized assurance frameworks. We request the Bank to accept SOC 2 Type II/ISO 27001 or equivalent independent assurance in lieu of a mandatory CERT-In-empanelled audit of the OEM's internal log-generation/storage/review process. " The OEM shall maintain documented security logging, monitoring, retention and review controls. Effectiveness shall be evidenced through applicable independent third-party assurance reports/certifications such as SOC 2 Type II, ISO 27001 or equivalent. CERT-In-empanelled audit may be required only for bidder-managed components deployed specifically within the Bank environment, where applicable."	Please refer addendum for the revised clause
2579	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	82.5	IT Act 2000 & its amendments, and other Acts/Regulatory guidelines.	Kindly clarify that the OEM must comply with legal/regulatory requirements applicable to it as the provider of the proposed hosted service and provide reasonable documentation to support the Bank's compliance obligations. " OEM shall comply with applicable legal and regulatory obligations relevant to its provision of the proposed service and shall provide available security/privacy/compliance documentation reasonably required to support the Bank's applicable obligations."	Please refer addendum for the revised clause
2580	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	83	CERT IN Empaneled auditor report's is required for the following:	We request the Bank to permit internationally recognized independent assurance reports/certifications for OEM-managed hosted services. CERT-In empanelled audit reports may remain applicable to India-specific bidder-managed/on-premises components where such audit is feasible and required. " For OEM-managed hosted/SaaS services, independent assurance reports/certifications such as SOC 2 Type II, ISO 27001 or equivalent shall be accepted. CERT-In empanelled audit reports shall be applicable only to components/services for which such India-specific audit is contractually and technically feasible."	Please refer addendum for the revised clause
2581	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	92	The application and DB is/will be hosted separately on a dedicated infrastructure (physical/logical) for PSB. Evidence of dedicated infrastructure (physical/logical) for PSB should be submitted.	The proposed platform is an OEM-managed hosted security service designed with logical access controls and customer data isolation. Requiring dedicated physical application/database infrastructure would restrict standard SaaS/POD architectures without necessarily improving the security outcome. We request acceptance of secure logical tenant/customer isolation supported by independent assurance evidence. " The proposed hosted service shall provide secure logical segregation/isolation of Bank data and administrative access from other customers through appropriate access-control and tenant-isolation mechanisms. Dedicated physical application/database infrastructure shall not be mandatory where equivalent logical isolation is implemented and independently assured."	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2582	8	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	98.1	Feasibility to audit/review IT controls of the third party or obtaining independent review report for the same from CERT-In empaneled security consultant, to ensure it meets Bank's information security requirement.	We request that the Bank permit review of current independent assurance reports/certifications as the primary mechanism for reviewing OEM IT controls. Any direct audit should remain subject to the OEM's standard contractual audit provisions, confidentiality, security, scope and advance-notice requirements." The Bank may review applicable independent third-party assurance reports/certifications covering the hosted service. Where additional audit is required, such audit shall be subject to mutually agreed scope, confidentiality/security restrictions, reasonable advance notice and the OEM's standard contractual audit provisions. A CERT-In empanelled consultant may review evidence made available under these conditions."	Please refer addendum for the revised clause
2583	Appendix 1A Page 40	NDR Functional Compliance Sheet	Clause 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high- availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	The Clause mandates Cloud based SaaS model, while RFP Page 30, Page 35, section 7.2.4.1 clause 'd' asks for on Premesis solution "The NDR shall be deployed On-Premises". We request to modify the clause to include On-Prem solution. Justification: To include solutions which are on-Prem based	Please refer Addendum for revised clause
2584	Appendix 1A Page 40	NDR Functional Compliance Sheet	Clause 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high- availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	The Clause asks for Active-Active HA architecture, we request to include Active-Standby Mode. Justification: Management Console is central console, it cannot be deployed in Active-Active mode, as it is a central component.	Please refer Addendum for revised clause
2585	Appendix 1A Page 41	NDR Functional Compliance Sheet	Clause 18	Solution should have the capabilities to create and run security playbooks for automation and better MTTD/MTTR on the basis of criticality of threat/server	Proposed solution adopts below appraoch for automated MTTD, Solution need investigative workflows and all the alerts need to be validated before building any Active Response Solution is having inbuilt playbooks like Host, Session and Packet analysis. once alert is validated Active Response can be triggered. Hope the approach is acceptable	Yes, your understanding is correct Also, Please refer addendum for the revised clause
2586	Page 66	7.6.7	Training	At a minimum, the following training programs shall be conducted for each proposed solution / OEM appointed officials: Duration per Session and Munimum Number of Sessions	Overall there is a requirement of 15 Sessions and Duration per session is 2 or 3 days. This takes the total training per solution to 40 days. This is very large reqirement of training, we request to make it to 3 days for NDR solution	Please refer addendum for revised clause
2587	Page 63	7.6.6	Testing, clause 3	The bidder shall provision and maintain dedicated Development, Testing, UAT, and Pre-Production environments throughout the contract period.	Is UAT Environment required for NDR solution also, given that NDR is a Passive and out of path solution.	Please refer addendum for revised clause
2588	30, 34	7.2.1 Deployment Model & HA (TIP) / 7.2.4.1 Deployment Pattern	Table 7.2.1 Sr. 7; Cl. 7.2.4.1(e)	"Threat Intelligence Platform (TIP) - Cloud (SaaS) + Hybrid - Bank Location: Broker/Collector/Integrator: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR" (Table 7.2.1).	Cyble's Threat Intelligence Platform (TIP) is delivered as a fully cloud-native SaaS solution, providing continuous threat-intelligence aggregation, enrichment and distribution to the Bank via API, STIX/TAXII feed and a dedicated web portal, with high availability, geographic resiliency and disaster recovery built into the SaaS platform itself - fully aligned with the SLA, RTO and RPO defined in Section 13. As the TIP's core function requires no packet-level or in-line processing within the Bank's network, Cyble can meet the Bank's continuity requirement for this solution without deploying a broker/collector component on Bank premises. We request the Bank's confirmation that this cloud-native delivery model will be accepted as fully compliant with Table 7.2.1.	Please refer addendum for the revised deployment requirement
2589	31, 35	7.2.1 Deployment Model & HA (CSPM) / 7.2.4.1 Deployment Pattern	Table 7.2.1 Sr. 11; Cl. 7.2.4.1(i)	"Cloud Security Posture Management (CSPM) - Cloud (SaaS) + Hybrid - Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR" (Table 7.2.1); "...with the required connectors, collectors, agents, enforcers and/or other supporting Bank-side components, if required, deployed at the Bank's DC and DR in N+N Active-Active configuration" (Cl. 7.2.4.1(i)).	Cyble's Cloud Security Posture Management (CSPM) module continuously assesses the Bank's cloud environments through secure, read-only, API-based/cross-account IAM-role integration, with no agent, connector or collector required on Bank premises. This lets Cyble deliver continuous, real-time cloud security posture monitoring with high availability and resilience built natively into the SaaS platform, fully meeting the Bank's SLA, RTO and RPO requirements under Section 13. This is consistent with the qualifying language "if required" already present in Cl. 7.2.4.1(i). We request the Bank's confirmation that this API-integrated, cloud-native delivery model will be accepted as compliant.	Please refer addendum for the revised clause
2590	55-56	7.4.3 Attack Surface Management	Cl. 7.4.3	"Discovery of internet-facing and internal assets... The proposed solution shall provide AI-enabled Attack Surface Management (ASM) capabilities for continuous discovery... of the organization's external attack surface, including known and unknown internet-facing assets."	Cyble's Attack Surface Management (ASM) capability provides continuous, AI-enabled discovery, monitoring and risk-prioritization of the Bank's entire external attack surface - internet-facing assets, exposed services, domains, cloud assets and shadow IT - using external/passive reconnaissance together with Bank-shared asset inventories (IP ranges, domains, cloud accounts), with no agent or appliance required inside the Bank's network, consistent with the offsite Managed Service model in Section 7.2.2. This gives the Bank a complete outside-in exposure view from Day 1. We request the Bank's confirmation that this externally-led, agentless approach satisfies Cl. 7.4.3.	Bank is looking for external attack surface management
2591	55	7.4.5 Anti-Phishing	Cl. 7.4.5	"...offsite continuous anti-phishing monitoring and response services for detection, analysis for phishing attacks targeting the Bank, its employees, customers, executives, digital assets, domains, and online channels."	Cyble is fully equipped to deliver continuous, 24x7 Anti-Phishing monitoring across the Bank's domains, executives and digital channels from Day 1 of the engagement, scaling seamlessly as the Bank's digital footprint grows, with no additional infrastructure required from the Bank. To finalise the onboarding plan, we request the Bank share the number of primary/registered domains, sub-domains, executive/VIP identities and customer-facing digital channels to be covered at contract commencement, so Cyble can confirm precise sizing against this scope.	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2592	57	7.4.6 Dark Web Monitoring	Cl. 7.4.6	"...offsite, tool-based continuous dark web and cyber threat exposure monitoring services... across the surface web, deep web, dark web, underground forums, messaging platforms, and data leak repositories."	Cyble's Dark Web & Cybercrime Monitoring capability continuously covers the surface web, deep web, dark web, underground forums, messaging platforms and data-leak repositories, and can begin protecting the Bank's specified identities, brand keywords and domains immediately upon contract signature. To tailor this coverage precisely, we request the Bank share the initial monitoring scope (employee/executive identities, brand keywords, domains and relevant data categories) so Cyble can confirm sizing and reporting cadence.	Details shall be shared with succesful bidder
2593	57	7.4.7 Threat Intelligence Feed	Cl. 7.4.7(l)	"Provision of threat intelligence through a centralized portal/dashboard and/or machine-readable feeds."	Cyble's Threat Intelligence Feed is delivered through both a centralized portal/dashboard and machine-readable, standards-based feeds (STIX/TAXII, MISP-compatible formats and API), enabling seamless integration with the Bank's existing or future security stack whenever required. We confirm this dual delivery model - portal-based consumption plus machine-readable feed/API - and request the Bank's confirmation that it satisfies Cl. 7.4.7.	No Change, Please be guided by the RFP
2594	57-58	7.4.8 Threat Hunting Services	Cl. 7.4.8(m)	"The threat hunting service shall be delivered remotely/offsite using secure and mutually agreed mechanisms for accessing relevant logs, telemetry, security tools, and data made available by the Bank."	Cyble can deliver proactive, intelligence-driven Threat Hunting entirely offsite - correlating curated external threat intelligence (IOCs, IOAs, TTPs, threat-actor and campaign intelligence) against Bank-shared context, supplemented by secure, mutually agreed read-only access to relevant Bank telemetry for validation and deeper investigation as needed - fully consistent with the remote/offsite delivery model mandated in Cl. 7.4.8(m). We request the Bank's confirmation that this intelligence-led hunting model, combined with agreed read-only telemetry access, meets the Bank's requirement.	No Change, Please be guided by the RFP
2595	58	7.4.9 Brand Protection and Monitoring	Cl. 7.4.9(j)	"Takedown coordination with relevant registrars, hosting providers, platforms, application stores, social media platforms, and other relevant entities, wherever applicable."	Cyble's Brand Reputation Monitoring capability continuously identifies brand impersonation, typosquatting, phishing/fraudulent websites, fraudulent mobile apps and social-media impersonation, and actively coordinates takedown requests with registrars, hosting providers, app stores and social platforms on the Bank's behalf under a standard authorisation executed at contract signature - delivering a fully managed, end-to-end takedown process with minimal effort required from the Bank's team. We request the Bank's confirmation that this bidder-led takedown coordination model satisfies Cl. 7.4.9(j).	Please refer addendum for revised clause
2596	256	16.21 Annexure 21: Sizing/Volumetrics (gap for Offsite Services)	Annexure 21, Sizing table	Annexure 21's sizing table provides explicit volumetrics (EPS, endpoint counts, IPs, VPCs, etc.) for the 14 solutions under Section 7.3, but no equivalent executive/VIP count is specified for the offsite services that monitor executive exposure (Anti-Phishing - Cl. 7.4.5, Dark Web Monitoring - Cl. 7.4.6, Brand Protection - Cl. 7.4.9).	Cyble's Executive Monitoring and Digital Risk Protection capabilities can protect any number of the Bank's executives/VIPs from Day 1, with coverage scaled precisely to the Bank's requirement across Anti-Phishing, Dark Web Monitoring and Brand Protection. To finalise sizing, we request the Bank confirm the number of executives/VIPs (e.g., Board members, CXOs, senior management) to be brought under continuous monitoring at contract commencement.	Please refer to the relevant Addendum for updated specfications
2597	256	16.21 Annexure 21: Sizing/Volumetrics (gap for Offsite Services)	Annexure 21, Sizing table	As above - no domain/sub-domain count is specified for the offsite services that monitor the Bank's external digital footprint (Attack Surface Management - Cl. 7.4.3, Anti-Phishing - Cl. 7.4.5, Brand Protection - Cl. 7.4.9).	Cyble can bring any number of the Bank's domains and sub-domains under continuous monitoring across Attack Surface Management, Anti-Phishing and Brand Protection from Day 1. To finalise sizing, we request the Bank confirm the number of primary domains and sub-domains to be monitored at contract commencement, and the expected annual growth in this count.	details shall be shared with successful bidder
2598	54	7.4 Functional Requirement - Services (Offsite Services)	Cl. 7.4(d)	"The Bidder shall implement appropriate security controls, including data masking or tokenization for sensitive data, Role-Based Access Control (RBAC), Just-in-Time (JIT) privileged access, and comprehensive audit logging for all services delivered under this RFP." - no named-user/license count is specified for platform/dashboard access to the 9 offsite services.	Cyble's platform can be provisioned for any number of the Bank's analysts, CISO-office and compliance stakeholders who need dashboard access to the offsite services, with full role-based access control as required under Cl. 7.4(d). To size the commercial bid precisely, we request the Bank confirm the number of named analyst/console user licenses required for the Bank's teams to access Cyble's platform and reporting for the proposed offsite services.	details shall be shared with successful bidder
2599	55, 58	7.4.5 Anti-Phishing / 7.4.9 Brand Protection and Monitoring	Cl. 7.4.5; Cl. 7.4.9(j)	Neither clause, nor Annexure 21, specifies an expected volume of takedown actions per month/year for phishing sites, fraudulent domains, or fake social media/mobile app listings.	Cyble is fully equipped to execute takedown actions at whatever volume the Bank's threat exposure requires. To align commercial terms precisely with the Bank's risk profile, we request the Bank confirm the estimated number of takedown actions (phishing sites, fraudulent domains, fake social media/mobile app listings) expected per month under Anti-Phishing and Brand Protection.	Please refer to the relevant Addendum for updated specfications
2600	101	EVALUATION CRITERIA	Eligibility Evaluation Criteria	The bidder should have a minimum average turnover of INR 500 crore per annum in India during the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth.	We request you to please amend as below: The bidder should have a minimum average turnover of INR 250 crore per annum in India during the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth.	No Change, Please be guided by the RFP
2601	180	16.5 Annexure 5: Pre-Qualification Criteria		Documentary Proof for all eligibility criteria and Technical scoring under RFP clause "10.2 Eligibility Evaluation Criteria" and "10.3 Technical Evaluation Criteria"	Projects where the PO was awarded prior to 5 years for which Installation Report / Sign-off has been optained and the Project is completed in last 5 years from the PSB RFP publication date. For all such projects that are completed in all respect, customer may not issue any credential letter on current date, hence all earlier document issued should be accepted. If required, bidder's self-declaration can also be submitted stating the compliance to such criteria	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2602	181	16.5 Annexure 5: Pre-Qualification Criteria	7	The Bidder must have successfully supplied, installed and maintained (or under maintenance) SIEM Solution of minimum 20000 EPS / 0.86 TB per day in one PSU/ PSE/ Government Organizations / BFSI/Telecom provider in India in last 5 years Note: - A Bidder's experience shall be considered irrespective of when the implementation was completed. Even if the implementation was completed more than five years prior to the date of publication of the RFP, such experience shall qualify only where the same Bidder that supplied, installed and implemented the SIEM Solution is also currently maintaining the same solution, or has maintained the same solution at any time during the five-year period preceding the date of publication of the RFP.	We request bank to relax the sais criteria as under : The Bidder must have successfully supplied, installed and maintained (or under maintenance) SIEM Solution of minimum 15000 EPS / 0.6 TB per day in one PSU/ PSE/ Government Organizations / BFSI/Telecom provider in India in last 5 years Note: - A Bidder's experience shall be considered irrespective of when the implementation was completed. Even if the implementation was completed more than five years prior to the date of publication of the RFP, such experience shall qualify only where the same Bidder that supplied, installed and implemented the SIEM Solution is also currently maintaining the same solution, or has maintained the same solution at any time during the five-year period preceding the date of publication of the RFP.	Please refer addendum for revised clause.
2603	129	10.3 Technical Evaluation Criteria	1	Bidder should have supplied, installed and maintained (or under maintenance) the below solutions in any one PSU/PSE/ Government Organizations / BFSI/Telecom provider in India 1. SOAR 2. UEBA 3. Extended Detection & response (XDR)/ Endpoint Detection & response (EDR) 4. Network Detection & response (NDR) 5. Threat Intelligence Platform 6. Vulnerability Assessment / Vulnerability Management 7. Identity Threat Detection & response (ITDR) 8. Decoy/Honeypot/Deception 9. Application security testing tool (DAST/SAST) 10. CSPM	In line with eligibility criteria, we request to amend the clause as under : Bidder should have supplied, installed and maintained (or under maintenance) the below solutions in any one PSU/PSE/ Government Organizations / BFSI/Telecom provider in India 1. SOAR 2. UEBA 3. Extended Detection & response (XDR)/ Endpoint Detection & response (EDR) / **NBAD** 4. Network Detection & response (NDR) 5. Threat Intelligence Platform 6. Vulnerability Assessment / Vulnerability Management 7. Identity Threat Detection & response (ITDR) 8. Decoy/Honeypot/Deception 9. Application security testing tool (DAST/SAST) 10. CSPM	Please refer addendum for the revised clause
2604	129	10.3 Technical Evaluation Criteria	1	Bidder should have supplied, installed and maintained (or under maintenance) the below solutions in any one PSU/PSE/ Government Organizations / BFSI/Telecom provider in India 1. SOAR 2. UEBA 3. Extended Detection & response (XDR)/ Endpoint Detection & response (EDR) 4. Network Detection & response (NDR) 5. Threat Intelligence Platform 6. Vulnerability Assessment / Vulnerability Management 7. Identity Threat Detection & response (ITDR) 8. Decoy/Honeypot/Deception 9. Application security testing tool (DAST/SAST) 10. CSPM	As DAST / SAST is also provided as service to the customers, hence, we request you to kindly accept DAST / SAST experience on Services model as well	Please refer addendum for the revised clause
2605	129	10.3 Technical Evaluation Criteria		Documentary Proof for all Technical scoring under RFP clause "10.3 Technical Evaluation Criteria"	We understand that all the documentary evidences, including the "Notes" as asked in eligibility criteria will be applicable for Technical evaluation criteria also	Yes, your understanding is correct
2606	129	10.3 Technical Evaluation Criteria	1	Bidder should have supplied, installed and maintained (or under maintenance) the below solutions in any one PSU/PSE/ Government Organizations / BFSI/Telecom provider in India 1. SOAR 2. UEBA 3. Extended Detection & response (XDR)/ Endpoint Detection & response (EDR) 4. Network Detection & response (NDR) 5. Threat Intelligence Platform 6. Vulnerability Assessment / Vulnerability Management 7. Identity Threat Detection & response (ITDR) 8. Decoy/Honeypot/Deception 9. Application security testing tool (DAST/SAST) 10. CSPM Scoring Point 1: Experience in 3 solutions – 8 Marks Point 2: Experience in 4 solutions –10 Marks Point 3: Experience in 5 solutions –12 Marks Point 4: Experience in more than 5 solutions– 15 Marks Max Marks – 15 Marks	Request bank to kindly revise the scoring as under : Point 1: Experience in 3 solutions – 10 Marks Point 2: Experience in 4 solutions –12 Marks Point 3: Experience in 5 solutions –15 Marks Max Marks – 15 Marks	Please refer addendum for the revised clause
2607	137		11.1 Product (Software) Cost	Product License Cost - On successful delivery of the licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware - 50%	**Product License Cost** - On successful delivery of the licenses which would be considered delivered on submission of proof of delivery - 70%	No Change, Please be guided by the RFP
2608				On successful UAT Signoff of the respective product - 20%	On successful UAT Signoff of the respective product - 20%	No Change, Please be guided by the RFP
2609				On successful Go-live of the respective product - 30%	On successful Go-live of the respective product - 10%	No Change, Please be guided by the RFP
2610				Product Implementation Cost - On Successful installation of OOTB product on the sourced hardware and handing over the environment with OOTB product to Bank - 20%	**Product Implementation Cost -** On Successful installation of OOTB product on the sourced hardware and handing over the environment with OOTB product to Bank - 50%	No Change, Please be guided by the RFP
2611				On successful UAT Signoff of the respective product - 50%	On successful UAT Signoff of the respective product - 30%	No Change, Please be guided by the RFP
2612				On successful Go-live of the respective product - 20%	On successful Go-live of the respective product - 10%	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2613				Within 3 months of successful Go-live - 10%	Within 3 months of successful Go-live - 10%	No Change, Please be guided by the RFP
2614				Subscription Cost (One time license Cost) On successful delivery of the Licenses which would be considered delivered once the software (with OOTB features) is made available for view and review of the bank on the proposed hardware - 50%	**Subscription Cost (One time license Cost) for Year-1** On successful delivery of the licenses which would be considered delivered on submission of proof of delivery - 70%	No Change, Please be guided by the RFP
2615				On successful UAT Signoff of the respective product - 20%	On successful UAT Signoff of the respective product - 20%	No Change, Please be guided by the RFP
2616				On successful Go-live of the respective product - 30%	On successful Go-live of the respective product - 10%	No Change, Please be guided by the RFP
2617	138	11 PAYMENT TERMS	11.3 Hardware Cost	Appliance Cost On successful Delivery of the Appliance which would be considered delivered once the solution (with OOTB features) is made available for view and review of the bank. - 50%	**Appliance Cost** On successful delivery of the licenses which would be considered delivered on submission of proof of delivery - 70%	No Change, Please be guided by the RFP
2618				On successful UAT Signoff of the respective product - 20%	On successful UAT Signoff of the respective product - 20%	No Change, Please be guided by the RFP
2619				On successful Go-live of the respective product - 30%	On successful Go-live of the respective product - 10%	No Change, Please be guided by the RFP
2620				Hardware Cost (Other than Appliances) Delivery (power on) of hardware and submission of invoice with Proof of Delivery and other documents of the hardware supplied. - 70%	**Hardware Cost (Other than Appliances)** Delivery (power on) of hardware and submission of invoice with Proof of Delivery and other documents of the hardware supplied. - 70%	No Change, Please be guided by the RFP
2621				On successful installation of proposed solutions on the hardware - 50% of the sought product/solutions - 15%	On successful installation of proposed solutions on the hardware - 50% of the sought product/solutions - 20%	No Change, Please be guided by the RFP
2622				On successful installation of remaining proposed solution on the hardware – remaining 50% of the sought product/solutions - 15%	On successful installation of remaining proposed solution on the hardware – remaining 50% of the sought product/solutions - 10%	No Change, Please be guided by the RFP
2623	139	11 PAYMENT TERMS	11.4 ATS/subscription cost & AMC Cost	ATS/ Annual Subscription & Appliance AMC Cost Yearly in advance (Post submission of 110% of Annual subscription cost in the form of Bank Guarantee of the respective product) or quarterly in arrears	As per the RFP, bidder would be submitting a PBG for 5% of the overall Project value, which would include AMC/ATS amount as well, hence, we request bank to waive-off this additional Bank Guarantee	No Change, Please be guided by the RFP
2624				Appliance AMC - Yearly in advance (Post submission of 110% of the yearly AMC Amount of the respective product in the form bank guarantee) or quarterly in arrears	As per the RFP, bidder would be submitting a PBG for 5% of the overall Project value, which would include AMC/ATS amount as well, hence, we request bank to waive-off this additional Bank Guarantee	No Change, Please be guided by the RFP
2625	139	11 PAYMENT TERMS	Product (Software) Cost, Appliance cost, Hardware Cost, Implementation Cost and ATS/subscription cost & AMC Cost		Since, this RFP has multiple Product & Solutions, hence, we understand that the milestones, sign-off and payment terms will be individually considered for each product & Solution.	No Change, Please be guided by the RFP
2626	139	11 PAYMENT TERMS	Product (Software) Cost, Appliance Cost and Hardware Cost		We request bank to clarify the difference between the above stated 2 milestones - installation of OOTB product on the sourced hardware and handing over the environment with OOTB product to Bank and UAT sign-off. As per our understanding OOTB will be completed once the UAT is sign-off by bank.	No Change, Please be guided by the RFP
2627	98	9 PROJECT TIMELINES	Overall Implementation period shall be 5 Months (Start Date is T0) for all solution & services	The bidder shall submit a comprehensive Project Plan, within 7 days of T0 covering each proposed product/solution & Services, detailing all project phases, milestones, tasks, sub-tasks, activities, timelines, dependencies. The bidder shall submit the detailed Project Plan within seven (7) days from T0 for the Bank's review and approval. Any Liquidated Damages (LD) for delays in project execution shall be calculated based on the bank's approved Project Plan. In the event the bidder fails to submit the Project Plan within seven (7) days from T0, the Bank reserves the right to levy applicable Liquidated Damages for each day of such delay. If the delay in submission of project plan exceeds seven (7) days, the Bank may prepare and issue the Project Plan, which shall be final and binding on the bidder. The bidder shall execute the project in accordance with the Bank-issued Project Plan, maintaining the overall implementation period of five (5) months from T0. All applicable Service Level Agreements (SLAs), milestones, Liquidated Damages (LDs), and other contractual obligations shall thereafter be governed by the Bank-issued Project Plan, which shall be deemed to have been accepted by the bidder without any further objection or reservation	Bank has not provided milestione-wise Project timelines, hence, we understand that LD / Penaties will be considered on overall implementation / sign-off of the Project. Also comsidering the comprehensiveness of the Project, we request bank to allow overall implementgation period of 7 months.	No Change, Please be guided by the RFP
2628	Page | 141	13.1 Service Level Agreement	Clause 16 - Critical Firewall/CBS incident additional penalty	Critical Firewall / Perimeter Firewall incident penalty	Clause 16 imposes an additional penalty (0.5% of MMC per hour beyond 120 minutes) where a Critical-Level Incident on the Core/Perimeter Firewall disrupts CBS or other critical banking services. Kindly clarify whether this additional penalty is over and above the standard Availability/Service-Level SLA penalty already applicable for the same incident, or whether only the higher of the two penalties shall be levied, to avoid double penalization for a single incident.	Please refer addendum for revised clause.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2629	Page | 142	13.1 Service Level Agreement	Clause 17 - RCA submission penalty (Rs.20,000/day)	RCA submission delay penalty	The RCA report is required to be 'issued by the respective OEM' within 3 working days of incident resolution, failing which a penalty of Rs.20,000/calendar day is levied on the bidder. Since RCA turnaround time is largely controlled by the OEM and not the bidder, request the Bank to provide relief/extension to the bidder where the delay is demonstrably attributable to the OEM, subject to the bidder having escalated in a timely manner or extend the 3 working days to atleast 7 working days as OEM having different level of approvals for sharing RCAs and redue the penalty amount to Rs. 10,000/-day.	No Change, Please be guided by the RFP
2630	Page | 146	13.1 Service Level Agreement - Availability Measurements	Monthly/Quarterly Maintenance Cost (MMC) formula	MMC calculation formula clarification	The formula for Monthly Maintenance Cost divides the sum of FM Manpower Cost, AMC and ATS/Subscription cost by '60', and the Quarterly formula divides the same by '20'. Kindly clarify/confirm the basis of these divisors (e.g., whether these represent number of months/quarters over the 5-year 6-month contract tenure) as the formula as drafted is ambiguous and may lead to disputes in penalty computation.	No Change, Please be guided by the RFP
2631	Page | 151-152	13.1 Service Level Agreement - Manpower Availability	Penalty of Rs.25,000 per resource per week or part thereof	Definition of 'week' and pro-ration of manpower shortfall penalty	Kindly clarify: (a) whether 'week' for this penalty means a fixed calendar week (Mon-Sun) or any rolling 7-day period from the date of shortfall; and (b) whether the penalty is levied on a pro-rata/per-shift basis for a partial-day shortfall (e.g., a resource on short leave and replaced within the same shift) or only for shortfalls persisting across a full day/week.	No Change, Please be guided by the RFP
2632	Page | 151-152 / Page | 75	13.1 SLA (Manpower Availability) read with 7.12.5	Interplay between resource-replacement transition timelines and Manpower Availability penalty	Relief during Bank-approved resource transition period	Section 7.12.5(7) allows a transition/knowledge-transfer period of 45 days (L1/L2) and 60 days (PM/L3) for resource replacement, subject to Bank approval. Kindly confirm whether the Manpower Availability penalty is held in abeyance during such Bank-approved transition periods (where the incoming resource is being onboarded per process), or whether the penalty applies from Day 1 of vacancy notwithstanding a compliant, Bank-approved replacement process. We request to amend this for L1 - 15 days, L2-30 days and L3/PM-45 days.	No Change, Please be guided by the RFP
2633	Page | 151	13.1 SLA - Deployment and Retention of Key Resources	Definition of 'Key Resources'	Scope of 'Key Resources'	Please define/confirm the roles to be treated as 'Key Resources' for the purpose of the Rs.2,00,000 per-instance penalty on unauthorized replacement - specifically, whether this is limited to the Project Manager/L3, or also extends to L1/L2 resources.	No Change, Please be guided by the RFP
2634	Page | 75	7.12.4 Minimum Resource Count Deployment	Shift-wise minimum L1/L2/L3 table	Tower-wise vs aggregate minimum manpower	The minimum resource table specifies a single set of L1/L2/L3 counts per shift, without segregating requirement by technology tower (SIEM/SOAR, EDR/XDR, NDR, DLP, PIM/IDAM, Cloud Security, CASB, Anti-Phishing & Brand Monitoring, CART, Threat Intel, etc.). Kindly clarify whether the specified minimum (4 L1 / 2 L2 / 1 L3 per shift) is the aggregate across all in-scope towers, or whether tower-specific minimum staffing is additionally expected, as this materially affects sizing and commercial quoting.	The Resource requirement given in the RFP is minimum mandatory requirement that is to be deployed. It includes both DC & DR. Bidder can propose the manpower over and above if required.
2635	Page | 75	7.12.4 Minimum Resource Count Deployment - Note 2	Backup/replacement resources for 24x7x365 coverage	Dedicated vs shared backup manpower	Note 2 requires the bidder to factor 'adequate backup and replacement resources' to ensure uninterrupted 24x7x365 availability of the minimum table counts. Kindly clarify whether this backup capacity needs to be additional dedicated headcount over and above the table counts, or may be met through a shared/on-call/cross-trained resource pool.	No Change, Please be guided by the RFP
2636	Page | 75	7.12.3 / 7.12.5 Resource Management and Governance	Bank approval turnaround for resource replacement	Bank-side approval SLA for replacement resources	Since all resource replacement/redeployment requires prior written Bank approval, and non-availability of an approved resource is treated as an SLA breach (Manpower Availability Clause), kindly specify the maximum time within which the Bank shall interview/approve a replacement resource, so the bidder is not penalized for delays attributable to the Bank's approval process.	No Change, Please be guided by the RFP
2637	General	Section 13 / Section 14 (Terms and Conditions)	Exit Management / Transition-Out	Absence of Exit Management clause	The RFP does not appear to define an Exit Management/reverse-transition framework (timelines, handover obligations, continuation-of-service during transition, resource/documentation handover to an incoming vendor) applicable at contract end, expiry, or termination. Kindly confirm if a separate Exit Management SLA/clause will be issued via corrigendum, including definition of the transition-out period and the bidder's obligations during that period.	Please refer addendum for revised clause
2638	Page | 158	13.3 At-Risk Amount	Mechanism and applicability of At-Risk Amount	At-Risk Amount trigger and relationship to 10% penalty cap	Clause 13.3 states the monthly At-Risk Amount shall be 15% of the estimated monthly payout but does not describe the mechanism/trigger for withholding or recovering it, or its relationship with the penalty computations under Section 13.1. Kindly clarify (a) whether the At-Risk Amount is a withholding released upon compliance, or an additional penalty; and (b) whether recovery under the At-Risk Amount counts towards, or is over and above, the overall 10% penalty cap defined in Section 13.2.	The At-Risk Amount is a contractual performance mechanism and shall be withheld/adjusted in accordance with the applicable performance requirements specified in the RFP. It shall not automatically be treated as an additional penalty or Liquidated Damages (LD). Any withholding, adjustment or recovery under the At-Risk Amount shall be accounted for within the overall 10% penalty/LD cap specified in Section 13.2 and shall not be over and above such cap.
2639	Page | 143	13.1 SLA - Criticality Table	Uniform 15-minute response time across severities	Response time not differentiated by severity	The Response Time of 'within 15 minutes' is uniformly specified for Critical/High, Key/Medium, and Significant/Low severities, with only Resolution Time varying. Kindly confirm this is intentional, i.e., response time is common across all severities and does not vary with incident criticality.	No Change, Please be guided by the RFP
2640	Page | 141	13.1 Service Level Agreement - Clause 13	4-hour hardware repair/replace/standby requirement	Applicability of 4-hour hardware SLA at all locations	Kindly clarify whether the 4-hour repair/replace/standby requirement for non-functional critical hardware components applies uniformly across all deployment locations (SOC Office, DC, DR Site, and Branches, as referenced in Section 7.12.5), and if branch locations are included, whether a differential SLA/travel-time buffer will be permitted given logistics and spares-inventory constraints at dispersed locations.	The SLA shall apply to locations/components covered by the relevant RFP requirement. The bidder shall provide appropriate spares/logistics arrangements to meet the SLA.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2641	Page | 159	14.1 Assignment & Subcontracting	OEM personnel vs subcontracting	Treatment of OEM resources under the no-subcontracting clause	Clause 14.1 excludes 'Proposed OEM personnel' from the general prohibition on subcontracting. Kindly confirm that OEM resources deployed for specific product support (as distinct from the bidder's own onsite L1/L2/L3 staff) are not construed as impermissible subcontracting, and clarify the documentation the bidder must maintain to demonstrate that such OEM personnel are directly engaged by the OEM.	No Change, Please be guided by the RFP
2642	Page | 72-75	7.12.1 Implementation Phase / 7.12.4 O&M Phase	Effective start date of mandatory minimum manpower deployment	Commencement trigger for Manpower Availability SLA	Please confirm the effective date from which the mandatory minimum onsite O&M manpower deployment (and the consequent Manpower Availability SLA) becomes applicable - i.e., from Contract signing/LOI, or from the 'date of NextGEN SOC solutions installation' as referenced in Section 7.12.4 - given that implementation and staggered hardware delivery may span several months.	No Change, Please be guided by the RFP
2643	30	RFP - 7.2 Solution & Services Deployment Model and Their HA Requirement 7.2.1 Solutions – Master Deployment Matrix	6. Network Detection & Response (NDR)	Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Management Console: Deployed at both DC and DR	Different NDR solution works on different redundancy deployment methodology (I.e Active - Active or Active - Passive). Request bank to modify the clause as: Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active/Passive at DC and HA, N+N, Active-Active/Passive at DR. Management Console: Deployed at both DC and DR	Please refer addendum for the revised deployment requirement
2644	45	RFP - Scope of Work 7.3.5 Network detection and response (NDR)	7.3.5.1 Modules, Architecture & Deployment:	Pt 2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Generally NDR solutions are deployed with sole purpose of doing network analysis, threat detection & response and does not have native 2FA capability, so request bank to remove this point. As an alternate as proposed in same point, proposed NDR solution can be integrated with bank's existing MFA solution.	Please refer addendum for the revised clause
2645	49	RFP - Scope of Work 7.3.10 Application security testing Tool	7.3.10.1 Modules, Architecture & Deployment:	Pt 2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Generally AST solutions are deployed with sole purpose of scanning the source code, web, api etc and does not have native 2FA capability, so request bank to remove this point. As an alternate as proposed in same point, proposed AST solution can be integrated with bank's existing MFA solution.	No Change, Please be guided by the RFP
2646	110	RFP - 10.2 Eligibility Evaluation Criteria	OEM Evaluation Criteria	Pt 19. The proposed OEM SIEM Solution with a minimum capacity of 30,000 EPS or 1.2 TB/day shall have been successfully implemented on cloud in one (1) in India.	For wider participation, we request bank to amend the clause as: The proposed OEM SIEM Solution with a minimum capacity of 5,000 EPS or .2 TB/day shall have been successfully implemented on cloud in any one (1) Govt/PSU customer in India. OR The proposed OEM SIEM Solution with a minimum capacity of 10,000 EPS or .4 TB/day shall have been successfully implemented on cloud in one (1) in India.	Please refer addendum for revised clause.
2647	112	RFP - 10.2 Eligibility Evaluation Criteria	OEM Evaluation Criteria	Pt 20. The proposed OEM solution should have been implemented in at least one BFSI is to be submitted for the following solutions: NDR	For wider participation, we request bank to amend the clause as: The proposed OEM solution should have been implemented in at least one BFSI / Govt is to be submitted for the following solutions: NDR	Please refer addendum for the revised clause
2648	260	RFP - 16.21.2 Volumetrics- Solution-wise Requirements	12. Application Security Testing Tool	All the inline components of the solution must operate in high availability mode. In the event of any component failure, the system should automatically initiate failovers within seconds, ensuring uninterrupted functionality without requiring manual intervention.	Application Security Testing as a technology in general works at developemnt/pre-production/UAT stage only. And hence as a solution there is no need of high availability mode. Same has already been updated in this RFP (as solution is asked in standalone at both DC & DR). So, request bank to deleted this clause.	No Change, Please be guided by the RFP. The bidder must design the solution to fully comply with the RFP requirements, ensuring that in case of a failover, the system meets the defined SLA for availability, RTO, and RPO. The bidder is required to adhere to the deployment requirements outlined in the RFP when designing and proposing the solution architecture.
2649	40	APPENDIX 1A Functional Compliance Sheet (Solutions)	Network Detection & Response (NDR)	Pt 13. The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	As bank has asked for on-premise solution for NDR, on the contrary, this clause asks for cloud-native SAAS ask. So, we kindly request bank to delete this clause.	Please refer Addendum for revised clause
2650	42	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 3. The solution must be able to analyse a wide array of programming languages including Java,.Net, C/C++, Objective-C, Android, PHP, COBOL, Ruby, Swift, HTML 5, Scala, APEX, TypeScript, Go, Kotlin and ABAP etc but not limited to these alone	Considering the future requirements of AI in Secure Code Development and most of the development is moving towards AI generated code using AI supported languages. So it is very important for bank to have coverage around this as well and will recommend to incorporate AI supported languages like "R, Ada, Solidity, Bash, Groovy, Rust, Perl", but not limited to these alone.	No Change, Please be guided by the RFP
2651	42	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 24. Solution should support Machine learning and Analysis based on the archived results	ML capability is important, but it is very important to have coverage around AI based code as well. And will recommend bank to consider: The solution should have the capability to scan AI generated code. The solution should be able to integrate with AI coding agent via MCP	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2652	43	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 32. The solution should be able to support Composition Analysis: Identify the opens source components used in the application. Vulnerabilities & outdated version Licensing risk associated with the components	Bank is looking for Software composition analysis and asked for identifying the open source component and licensing risk. But this limited information is not enough for bank to secure themselves with rapidly increasing supply chain attacks and we will highly recommend to consider following as well: SCA system must catalogue open source components from Maven, NPM, and Nuget. SCA system has to be able to generate a Bill of Materials for an application. Solution should have the ability to continuously monitor the scanned components & notify if there are any zero day attacks without performing the rescan. Solution should Catalog, Store, and Audit SBOMs (both cycloneDx & SPDX) generated for in-house developed software applications and COTS applications.	No Change, Please be guided by the RFP
2653	5	1	Primary Storage	Proposed storage solution should be offerred with minimum 2 controllers with minimum 256 GB DRAM Cache memory on the entire storage Solution. The solution should scale to atleast 512GB Cache memory by adding additional controller.	**Change To:** Proposed storage solution should be offerred with minimum 2 controllers with minimum **128 GB DRAM** Cache memory on the entire storage Solution. The solution should scale to atleast **256GB Cache memory** by adding additional controller. **Explaination:** Cache ask should be Reduced as cache of 64GB or less per controller (128GB total) is enough as the latest CPUs, high-speed memory, and Gen 5 PCIe cards deliver the required performance efficiently. Modern storage controllers optimize cache usage, and industry benchmarks confirm that asked performance can be achieved with lower memory. This reduction not only meets technical needs but also decreases hardware, power, and cooling costs, resulting in a lower TCO for the solution	No Change, Please be guided by the RFP
2654	16	1	Backup Solution	The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data over a secure, API-based disk-to- disk (D2D) connection.	**Change To:** The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data **using standard Data protocolos such as FC, ISCI, NFS, S3** **Expalination:** This specific ask qulifies only specific backup appliance not any target storage as enterprise storage do not support data ingestion using API rather laverage protocols such as FC, ISCI, NFS , S3.	Please refer addendum for revised clause.
2655	25	1	Backup Solution	The Proposed Appliance/Backup Storage must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism	**Change To:**The Proposed Appliance/Backup **Solution** must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism **Explaination:** Proposed ask should be from Solution instead of storage as any storage does not offer file-level checksum reporting for backup files. This is typically a function of the backup software (e.g., Commvault, Veeam) that stores backups on storage.	Please refer addendum for revised clause.
2656	21	1	Primary Storage	If the OEM proposes effective storage capacity, then DRR should be applicable for the entire contract period. Incase, the DRR is not achieved anytime during the contract period, the OEM is liable to supply the additional drives/capacity to meet the required performance and effective capacity at no additional cost to the bank.	**Query :**Bank should provide workload details such as if data would encrypted or non-encrypeted , compressed or non-compressed and type of DB, VM etc. **Explaniation:** It would help OEM to size solution with correct DRR commitment.	Bidder/OEM shall assess the workload details and other relevant technical requirements and propose a suitably sized and architected solution meeting all requirements & terms of the RFP. The Bidder/OEM shall be responsible for sizing, performance, interoperability and adequacy of the proposed solution
2657		1	Long Term Storage	Addititional Point Request	**Point to be written as:** Long Term Storage should support WORM (Wrte Once, Read Many) capability to have Data Immutability. **Explaination:** We recommend implementing WORM (Write Once, Read Many) capability for long-term backup storage to ensure data is protected against accidental deletion and ransomware attacks. Additionally, WORM functionality is required to comply with regulatory guidelines for banking institutions. Since backup storage is expected to provide WORM capability, long-term backup storage should also comply with this requirement to maintain robust data protection .	As per tender pg no. 39, point a, *"No Bank data shall be deleted or made inaccessible before expiry of the applicable retention period (refer annexure 21) and without explicit written authorization from the Bank"* It is bidders responsibility to ensure that they comply with the tender requirement
2658		1	Primary Storage Backup Storage Long Term Storage	New Point request	**Point to be written as:** The proposed storage systems (for all 3 storage requirements), should have launch dates within past 3 years **Explainations:** We recommend qualifying storage systems with a launch date within the past three years. This approach ensures a better return on investment and reliable long-term support for a period of 7 to 10 years, as required by the bank. Some OEMs are currently offering systems that are over six years old and lack a clear roadmap or support commitment, which poses a risk to long-term operational stability and longitivity.	Please refer addendum for revised clause.
2659	29	7.2.1 Solutions – Master Deployment Matrix	Deception Technology (Decoy/Honeypot) -- HA Requirement	(Decoy/Honeypot)Bank Location: Any agent/Enforcer/Deceptor Standalone at DC and HA, N+N, Standalone at DR. Cloud (SaaS): Standalone Deployment aligned with the SLA, RTO & RPO (Refer Section 13).	Kindly confirm HA or standalone required in DC & DR	Please refer addendum for revised clause.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2660	31	7.2.1 Solutions – Master Deployment Matrix	HA Requirement	Note: For solutions deployed in Cloud (SaaS) + Hybrid mode, any agents, sensors, collectors, connectors, brokers, aggregators, gateways, enforcement components or other components required to be deployed within the Bank's infrastructure for collection, processing, integration, monitoring or enforcement shall be provided, deployed, configured, maintained and supported by the Bidder/OEM as part of the proposed solution and shall be included in the quoted cost.	We understand that required infra (VM , switch) to deploy the solution the solution will be provided by bank	No Change, Please be guided by the RFP
2661	40	7.3.1.1 Modules, Architecture & Deployment:	7.3.1.1 Modules, Architecture & Deployment:	Support collection of logs and telemetry from, at a minimum:	Kindly provide the details of Third-party systems and services & custom applications	Details shall be shared with successful bidder
2662	40	7.3.1.1 Modules, Architecture & Deployment:	7.3.1.1 Modules, Architecture & Deployment:	The solution shall provide granular RBAC with integration with enterprise SSO/MFA and support segregation of access based on user roles and administrative privileges.	We understand that MFA will be provided by bank. Kindly confirm and provide the details of existing MFA solution	Details shall be shared with successful bidder
2663	50	7.3.11 Cloud Security (CSPM) Tool	7.3.11.1 Modules, Architecture & Deployment:	Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: CSPM.	Kindly provide the details of existing clouds	details shall be shared with successful bidder
2664	56	7.4.4 Phishing Simulation	7.4.4 Phishing Simulation	The Bidder shall provide offsite, tool-based phishing simulation services to assess employee awareness, measure the Bank's resilience against phishing attacks, and support continuous improvement of security awareness.	Kindly confirm the number of users for phising simulation	Please refer addendum for revised clause
2665	57	7.4.6 Dark Web Monitoring	7.4.6 Dark Web Monitoring	The Bidder shall provide offsite, tool-based continuous dark web and cyber threat exposure monitoring services to identify potential exposure of the Bank's sensitive information across the surface web, deep web, dark web, underground forums, messaging platforms, and data leak repositories.	Provide the number of domains and subdomains which need to be monitor.	Detailed domain and identity information shall be provided to the selected bidder on a need-to-know basis
2666	58	7.4.9 Brand Protection and Monitoring	7.4.9 Brand Protection and Monitoring	Executive and key-person impersonation monitoring.	Provide the number of Executive and key-person for the monitoring.	Please refer addendum for revised clause
2667	63	7.6.5 Deployment and Go-Live - Activities are to be performed by Respective Solution OEM (supported by bidder)	7.6.5 Deployment and Go-Live - Activities are to be performed by Respective Solution OEM (supported by bidder)	Prior to Go-Live, the solution shall undergo security validation activities, including VAPT, IS Audit, readiness assessments, identi□cation of security gaps and blind spots, risk remediation, and implementation of recommendations.	We understand that VAPT and audits will be done by bank and closer need to done by bidder. Kindly confirm	VAPT & IS Audit shall be perofrmed by bank/bank appouinted agency before the go-live
2668	73	7.12.2 Operations and Maintenance (O&M) Phase	7.12.2 Operations and Maintenance (O&M) Phase	The respective OEMs shall provide subject matter experts from the date of installation throughout the contract period to support operations, troubleshooting, optimization, upgrades, audits, vulnerability remediation, and major incidents.	Kindly confirm OEM SME require onsite of remote support can be provided	No Change, Please be guided by the RFP
2669	92	7.18.1 Compute Infrastructure	7.18.1 Compute Infrastructure	a) The non-production environments should have the same software and hardware setup as deployed in production environments meeting all RFP requirements.	Kindly confirm do we need to give HA in no-production environment also as in DC & DR.	Non-production wherever, proposed shall be the standalone environment
2670	117	10.2	Eligibility Criteria-Clause-22	The proposed OEM solution should have been implemented in at least one verifiable client in India. Credential is to be submitted for the following solutions: a. CNAPP b. CWPP c. CTEM	CTEM is a new framework and customers are still in evaluation/ Implementation phase. Suggested change Client in India or Global BFSI The proposed OEM solution should have been implemented in verifiable client in India or Global. Credential is to be submitted for each of the following solutions: 1. CNAPP 2. CWPP 3. CTEM	No Change, Please be guided by the RFP
2671	120	10.2	Eligibility Criteria-Clause-23	The proposed OEM services should have been implemented in at least one (1) PSU/ PSE/ Government Organizations / BFSI in India. Credential is to be submitted for the following services: 1. Breach Attack & Simulation 2. Continuous Automated Red Teaming 3. Attack surface management 4. Phishing simulation 5. Anti-phishing services 6. Dark web monitoring 7. Brand protection & monitoring 8. Threat Intelligence feed 9. Threat Hunting services	As the offsite services are specified under the functional compliance requirements and are expected to be provided by the bidder, the corresponding eligibility criteria should be assessed at the bidder level. Suggested Changes: The proposed bidder services (below mentioned to the services) should have been implemented by the bidder in in at least one verifiable client in India.	No Change, Please be guided by the RFP
2672	86	16	Technical Specs-Anti Phishing-	Solution must be able to seamlessly integrate with On-Prem Mail Gateways via Mail Transfer Agent (MTA) forwarding	Anti-Phishing is asked as a Managed service however MTA is a componentfor onprim SEG gateway Suggested Change: Solution must be able to seamlessly integrate with On-Prem Mail Gateways via API integration	Please refer to the relevant Addendum for updated specfications
2673	87	18.2	Technical Specs-Anti Phishing-	Solution must provide DoS protection and directory harvest attack protection to ensure the availability of email services	DOS Protection Is Typically the Responsibility of the hardware based Email Infrastructure or Secure Email Gateway or Firewall or dedicated DDOS protection Hence this clause should not fall under Anti-Phishing services Also, this feature Suggested Change: Remove this clause	Please refer to the relevant Addendum for updated specfications
2674	87	19.2	Technical Specs-Anti Phishing	Solution must be able to display HTML banners on email clients, automatically switching to plain text format if HTML is not supported, while also providing multilingual support based on the organization's language preferences. HTML banner content can be edited or customized by organization	The requirement appears to prescribe a specific notification mechanism (HTML banner insertion) rather than the intended security outcome of user awareness and phishing risk notification. Modern anti-phishing solutions may provide user alerts through native email client warnings, subject tagging, security indicators, API-based notifications, or other mechanisms without relying on HTML banner injection. Suggested Change: Remove the clause	Please refer to the relevant Addendum for updated specfications
2675	87	19.4	Technical Specs-Anti Phishing	Solution must offer multiple disposition options, including attachment stripping, delivery of notices to senders, and quarantine of the whole email	Delivery of notice is platform specific feature Suggested Change Solution must offer multiple disposition options, including attachment stripping, and quarantine of the whole email	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2676	87	19.5	Technical Specs-Anti Phishing	Solution must provide a "Safe Preview" capability for administrators to view detailed information of quarantined messages and decide necessary actions	Safe Preview is a broad term, it should relate to anti-phishing Suggested Change Solution must provide a "Safe Preview of links" capability for administrators to view detailed information of quarantined messages and decide necessary actions	Please refer to the relevant Addendum for updated specfications
2677	88	19.8	Technical Specs-Anti Phishing-	As part of the forensic collection, should include the capture of PowerShell history	The requirement appears to mandate a specific forensic artefact (PowerShell history) rather than the intended security objective of investigating PowerShell-based activity. Suggested Change As part of the forensic collection, should include the capture of PowerShell history or equivalent forensic mechanism	Please refer to the relevant Addendum for updated specfications
2678	88	19.17	Technical Specs-Anti Phishing-	Solution must provide detailed reporting covering system usage and other areas including global message summary, spam, virus and other rule actions to save administrator time and effort in the collection of data for status reports. Reports can be emailed (HTML), printed, or downloaded in CSV format for use with third party tools	Suggested Changes: Solution must provide detailed reporting covering system usage and other areas including global message summary, spam, virus and other rule actions to save administrator time and effort in the collection of data for status reports. Reports can be emailed (HTML), printed, or downloaded in CSV or PDF format for use with third party tools	Please refer to the relevant Addendum for updated specfications
2679	88	19.18	Technical Specs-Anti Phishing-	Solution must have capability for administrators to view reports containing detailed statistics covering emails processed, rejected emails, SMTP transactions, and communication flows	The requirement mandates visibility into SMTP transactions and communication flow analytics, which are traditionally functions of MTA,and may not have direct access in API-based or cloud-native anti-phishing solutions. Suggested Change Solution must have capability for administrators to view reports containing detailed statistics covering emails processed, rejected emails.	Please refer to the relevant Addendum for updated specfications
2680	89	19.37	Technical Specs-Anti Phishing-	Solution must support message classification management, including separate classifiers for spam, impersonation, bulk, phishing, adult, and malware messages, with the ability to set score thresholds per category.	The requirement mandates a specific detection architecture based on separate classifiers and per-category scoring thresholds. Modern email security and anti-phishing solutions increasingly leverage AI/ML models, behavioural analytics, graph intelligence, and composite risk engines that may not expose individual classifiers Suggested Change Solution must support message classification management, including separate classifiers for spam, impersonation, bulk, phishing and malware messages, with the ability to set score thresholds per category.	Please refer to the relevant Addendum for updated specfications
2681	89	19.41	Technical Specs-Anti Phishing	Solution must provide granular administrative controls to allow role-based access to each module and quarantine folder.	Modern cloud-native anti-phishing solutions implement administrative segregation through configurable RBAC, delegated administration, role groups, and permission-based access models, which may not necessarily expose permissions at the individual module or quarantine-folder level Suggested Change Solution must provide granular administrative controls to allow role-based access	Please refer to the relevant Addendum for updated specfications
2682	89	19.43	Technical Specs-Anti Phishing	Solution must support complicated mail routing requirements, including group-based routing based on user groups	The requirement appears to address email infrastructure and mail-flow routing capabilities rather than core anti-phishing or email threat protection functionality. Complex mail routing, transport rules, and group-based routing are typically implemented within the email platform Suggested Change Remove this clause, its not applicable	Please refer to the relevant Addendum for updated specfications
2683	89	19.5 0	Technical Specs-Anti Phishing	solution must support a range of routing behaviors and actions for different scenarios, allowing administrators to customize email handling based on specific needs and requirements.	The requirement is broad and appears to focus on email routing and mail-flow management capabilities, which are typically functions of the email infrastructure (Microsoft Exchange, Exchange Online Suggested Change Remove this clause, its not applicable	Please refer to the relevant Addendum for updated specfications
2684	90	19.51	Technical Specs-Anti Phishing	Solution must support for in outbound or inbound email including footer management Inserting one or more legal or compliance footers (e.g. disclaimer) Multi-language support Apply different filters based on email attributes or active directory attributes, Insert dynamic content to footer such as date, when to apply the footer in the message routing hops, Selectively apply based on policy / attribute or not apply if the email is s/mime encrypted or digitally signed, etc Apply signatures and disclaimers based on AD user groups	Footer management is vendor specific feature Suggested Change Remove the clause	Please refer to the relevant Addendum for updated specfications
2685	90	19.5 3	Technical Specs-Anti Phishing	Solution must allow end-users to receive customized email notifications based on domain name.	The clause prescribes a specific notification customization method (domain-based) that may not be supported by all modern cloud-native Anti-Phishing solution Suggested Change: Solution must allow end-users to receive customized email notifications based alerts, and awareness messages based on organizational policies	Please refer to the relevant Addendum for updated specfications
2686	90	19.5 7	Technical Specs-Anti Phishing	Solution must provide administrators with capabilities for email queue management	This feature is excahnge or onprim gateway specific. Suggested Change Remove the clause	Please refer to the relevant Addendum for updated specfications
2687	90	19.5 9	Technical Specs-Anti Phishing	Solution must support alerting the security team on all policies, quarantine folders, and queue thresholds	The clause is a gateway-specific alerting model based on quarantine folders and queue thresholds. Modern cloud-native email security solutions may not utilise traditional mail queues while still providing comprehensive alerting for security incidents, policy actions, quarantine events, and operational status Suggested Change Solution must support alerting the security team on all policies, quarantine folders, and queue thresholds or equivalent alerting mechanism	Please refer to the relevant Addendum for updated specfications
2688	90	19.6 2	Technical Specs-Anti Phishing	Solution must provide application and message routing troubleshooting tools with a message-tracing capability to facilitate help desk work	Message routing trobleshooting & message-tracing capabilities are part of exchange provider. Suggested Change Remove the clause	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2689	32	7.2.2 Services (Offsite)	7.2.2 – Sl. 4 Phishing Simulation; read with 7.4 (f) and Annexure 21	Phishing Simulation – Offsite; Delivery Model: Managed Service; Frequency: Quarterly; additional campaigns may be conducted based on Bank requirements. 7.4 (f): frequency and scope of each service shall be as specified in Annexure 21 – Sizing/Volumetrics.	Clause 7.2.2 fixes the frequency at 'Quarterly', whereas Appendix 1C (S.No. 5, 6 and 18) requires 'unlimited' users/campaigns with 'no restriction' on emails, calls and SMS, and S.No. 14 requires 100 employees per month for manual vishing. Annexure 21 (p.256–257) does not contain any volumetrics for this service although 7.4 (f) refers to it. For uniform sizing and pricing, Bank is requested to confirm: (a) the total number of employees / email IDs in scope (including contractual and outsourced staff) and the number of mobile numbers for smishing/vishing; (b) the number of departments, zones and branches to be reported on; (c) the baseline number of exercises per year for each of email phishing, quishing, smishing, vishing (automated and manual) and mobile phishing. Kindly confirm that 'unlimited' means unlimited campaigns for the licensed user base.	Please refer addendum for revised clause
2690	56	7.4.4 Phishing Simulation	7.4.4 (b), (i)	(b) Behavioural analysis of users' responses to simulated phishing campaigns. (i) AI based user behaviour and phishing susceptibility analysis.	Click and credential-submission counts alone indicate whether a user fell for a simulation, not why. To make behavioural analysis actionable, Bank is requested to augment the clause as follows: 'The platform shall identify the psychological trigger(s) used in each simulation (e.g., fear, urgency, greed, curiosity, authority, reward/helpfulness) and compute an emotion-wise vulnerability index for each user, each department and organisation-wide, with ranking of users and departments against each trigger, trend across successive campaigns and identification of repeat offenders across email/SMS/QR/voice vectors.' Kindly confirm whether this may be incorporated in the corrigendum.	No Change, Please be guided by the RFP
2691	56	7.4.4 Phishing Simulation	7.4.4 (c), (e)	(c) Department-wise and user-wise risk assessment. (e) Identification of high-risk users and trends.	Bank is requested to confirm that risk assessment is expected at three levels – user, department/location and organisation – and that a user-level risk score should aggregate results across all campaigns and vectors (email, SMS, QR, voice, mobile) together with training completion status, so that 'high-risk users' are identified on a cumulative basis rather than per campaign. Please also confirm the history (e.g., rolling 12 months / contract tenure) over which trends are to be reported.	The platform shall provide user-wise and department-wise risk assessment and identification of high-risk users and trends as required by the RFP. The Bidder shall propose the methodology and reporting period necessary to meet the stated requirement.
2692	56	7.4.4 Phishing Simulation	7.4.4 (g), (h)	(g) Dashboard-based visibility of campaign status, results, user responses, and risk metrics. (h) Generation of management and executive reports as required by the Bank.	Bank is requested to specify (i) the frequency of management/executive reports (per campaign, monthly, quarterly); (ii) whether reports are to be presented in person to Senior Management/Committee and the number of such presentations per year; and (iii) whether role-based dashboard access is required for department/zonal heads to view their own team's results only.	The Bidder shall provide dashboards and management/executive reports as required by the Bank. The Frequency of conducting the excerices is defined in the RFP
2693	56–57	7.4.4 Phishing Simulation vs 7.4.5–7.4.8	7.4.4 (j), (k), (l), (m)	(j) AI based detection and classification of phishing and impersonation threats. (k) AI based analysis and correlation of exposed credentials, data leaks and threat indicators. (l) AI based enrichment, correlation and prioritization of threat intelligence. (m) AI based behavioural analytics, anomaly detection and threat correlation.	Items (j)–(m) duplicate services that the Bank is separately subscribing under 7.4.5 Anti-Phishing (impersonation/phishing-threat detection), 7.4.6 Dark Web Monitoring (exposed credentials and data leaks), 7.4.7 Threat Intelligence Feed (enrichment, correlation and prioritisation) and 7.4.8 Threat Hunting (behavioural analytics and anomaly detection). Bank is requested to (a) confirm that under 7.4.4, item (j) is limited to automated analysis and classification of emails reported by employees through the 'Report Phishing' plugin (header, sender-reputation, URL and attachment analysis with a verdict on an administrator portal), and (k), (l) and (m) from 7.4.4 or mark them 'desirable', so that the phishing simulation OEM is not required to bundle DRP/TIP/UEBA capabilities already procured under other services.	No Change, Please be guided by the RFP
2694	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 1 & 19.4 (a)	The platform shall facilitate creation of phishing campaigns including QR code phishing which can be customized by bank. (Repeated verbatim at S.No. 19.4 (a).)	S.No. 1 and S.No. 19.4 (a) are identical. Bank is requested to confirm whether the requirement will be scored twice (10 + 10 marks) or one entry will be removed. Please also confirm whether QR-code simulations are to be delivered via email, printed posters/SMS, or both, and that per-user QR-scan events are to be captured and reported in the same manner as link-clicks.	No Change, Please be guided by the RFP
2695	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 2, 3, 17	In-built email templates based on banking environment, current events and previous successful attacks; creation of new templates; templates based on current threat landscape targeted to banking environment.	Bank is requested to indicate the minimum number of ready-to-use banking-specific templates expected on Day 1 (email, SMS, voice scripts, QR) and to confirm whether templates simulating Bank's own internal applications and communications (HRMS, CBS alerts, IT helpdesk, RBI/CERT-In advisories) are required. Please also confirm that both HTML and plain-text email templates should be supported and that the template editor should permit Bank users to build/customise templates without vendor dependency.	No Change, Please be guided by the RFP. Details shall be discussed and deliberated with successful bidder on case to case basis
2696	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 7	The platform shall have the capability to schedule the campaign for a future date and time.	Bank is requested to enhance the clause to read: 'The platform shall support immediate send, scheduling for a future date/time, delivery within a defined date/time window (e.g., business hours only) and randomised/staggered delivery intervals across recipients to simulate realistic attack patterns and avoid mass detection.' Kindly confirm.	No Change, Please be guided by the RFP.
2697	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 8 (read with Annexure 21, p.257)	The platform should have capability to install a plugin with the bank's email client for reporting of any phishing incident. Annexure 21 lists O365 among the Bank's applications.	Bank is requested to confirm: (a) that the corporate email platform is Microsoft 365 (Exchange Online) as indicated in Annexure 21, and whether any on-premise Exchange or other mail system also exists; (b) the clients on which the plugin must function (Outlook desktop, Outlook Web/OWA, Outlook mobile); (c) whether centralised deployment of the add-in through the M365 Admin Centre will be facilitated by Bank; and (d) whether the plugin is expected to report only simulated emails or also real suspicious emails received by employees.	1) Bank is using O365 2) The Bidder shall ensure integration with the Bank's email environment as required by the RFP. The Bidder shall assess the Bank's existing environment during implementation and provide all required integration/configuration support within its scope. 3) Bank will asisst in integration hwoeevr, end to end responsibility lies with the bidder/OEM 4) Bidder scope is limited to the propsoed services (Phishing Simulation)

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2698	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 8 (proposed enhancement)	(Same clause – proposed enhancement)	To ensure the 'Report Phishing' capability adds value to the Bank's SOC and not only to the simulation, Bank may consider amending the clause to include: 'The Report Phishing button shall (i) allow reporting of any suspicious email, whether or not generated by the platform; (ii) allow the user to indicate whether he/she recognised the email as phishing and add comments; (iii) forward the reported email with full headers to a Bank-designated mailbox (e.g., SOC/CISO cell); (iv) provide an administrator portal listing all reported emails with automated threat analysis; and (v) allow administrators to mark reported emails as reviewed/closed after investigation. Report-phishing metrics (reporting rate, time-to-report) shall be included in campaign reports.' Kindly confirm.	No Change, Please be guided by the RFP
2699	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 9	The platform should support English language for creating phishing templates. Support in other regional languages and Hindi would be an added advantage.	Bank is requested to specify the regional language(s) required (e.g., Punjabi) in addition to English and Hindi, and to confirm whether the multilingual requirement applies to (a) phishing email templates only, or also to (b) landing pages, (c) SMS/vishing scripts and (d) training content and quizzes. Please confirm whether regional-language support will be scored as mandatory or as an added advantage.	No Change, Please be guided by the RFP
2700	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 10	The platform should allow creation of multiple users for executing the campaigns.	Bank is requested to confirm the administrative roles required (e.g., Super Admin, Campaign Manager, Content/Training Admin, Read-only/Auditor, Department-level viewer) and the approximate number of administrator accounts, and whether administrator authentication is to be through the Bank's SSO/MFA as per 7.4 (e) (refer separate query).	The platform shall support multiple administrative users and appropriate role-based access control. The Bidder shall propose the required administrative roles and ensure secure access, including MFA/SSO integration where required by the RFP.
2701	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 11	The platform should support integration with bank's active directory.	Bank is requested to confirm: (a) whether the directory is on-premise Active Directory (LDAP/LDAPS), Microsoft Entra ID (Azure AD) or both; (b) the required synchronisation frequency; and (c) whether attributes such as department, location, designation and reporting manager are maintained in AD or must be sourced from HRMS/CSV. Bank may also consider adding: 'The platform shall support bulk onboarding through CSV import, automatic updating of user records on directory sync, duplicate detection during import/sync, and retention of historical campaign and training records when a user is disabled or deleted.'	No Change, Please be guided by the RFP
2702	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 12	The proposed solution should have incident management capabilities and same should be integrated with Bank's Incident Management solution.	Bank is requested to name the Incident Management / ITSM tool in use (e.g., ServiceNow, BMC Remedy, ManageEngine) and the integration mechanism available (REST API / email-to-ticket / webhook). Please also clarify what event constitutes an 'incident' for this purpose – an employee-reported suspicious email, a credential submission during simulation, or both – and whether ticket creation is to be automatic.	No Change, Please be guided by the RFP
2703	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 13	The platform should support integration with bank's security stack such as SIEM, SOAR, data lake etc., as per bank's requirement.	Bank is requested to confirm whether the SIEM / SOAR / data lake referred to are the NextGen SOC components being procured under this RFP or existing tools (please name); the integration method expected (Syslog/CEF, REST API); the event categories to be forwarded (campaign events, reported emails, administrator audit logs); and whether integration is required at Go-Live or 'as per Bank's requirement' during the contract. Bank may also confirm that no separate connector licence cost is to be quoted.	No Change, Please be guided by the RFP
2704	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 14	The bidder shall be capable of performing vishing exercises in both automated and manual methods … For manual approach, each exercise shall be targeted for 100 employees per month.	Bank is requested to clarify: (a) whether 'automated' vishing means IVR / pre-recorded voice calls placed through the bidder's telephony gateway, and 'manual' means live calls by trained human callers; (b) the total number of manual vishing exercises per year (100 employees per month implies 1,200 employees per annum – please confirm) and whether the 100 employees are unique each month; (c) that Bank will provide target telephone numbers and a written authorisation; and (d) whether call recordings are to be retained and shared with Bank, and the applicable retention period.	The Bidder shall comply with the requirement for manual Vishing as specified in the RFP. The Bidder shall describe its proposed methodology, resources and approach during technical bid
2705	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 14 (proposed enhancement)	(Same clause – proposed enhancement)	AI-voice / bot-based calling follows a fixed script and cannot adapt to the employee's responses, and therefore under-estimates real social-engineering risk. Bank may consider amending the clause to specify that 'manual vishing shall be conducted by trained human callers (not AI voice bots) using Bank-approved pretexts in the required languages, with the ability to adapt the conversation in real time, capture the employee's response and classify the outcome (e.g., disclosed information / refused / verified caller / reported).' Kindly confirm.	No Change, Please be guided by the RFP
2706	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 15	The bidder shall be capable to perform vishing activity in multiple regional languages, covering minimum English and Hindi.	Bank is requested to confirm the regional language(s) required for vishing callers in addition to English and Hindi (e.g., Punjabi), and the indicative proportion of calls in each language.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2707	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 16	The bidder shall conduct Smishing exercises … provide, maintain and manage an independent SMS gateway … maintain adequate security measures to protect Bank's data including any PII.	**Please refer addendum for revised clause** The Bidder shall assess the Bank's requirements. The proposed services should be integrated with bank's SMS gateway. The Bidder shall ensure compliance with all applicable statutory/regulatory requirements for SMS delivery in India. The SMS gateway shall be provided by the Bank. The bidder/OEM shall integrate its proposed solution with the Bank's SMS gateway. The bidder shall maintain adequate security measures to protect Bank's data including any PII information submitted by users during the activity. **Clarification**:The Bidder shall assess the Bank's requirements and size the SMS gateway/service accordingly. The required target population and frequency shall be as per Bank requirements during the contract period.	Please refer addendum for revised clause.
2708	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 16 (proposed enhancement)	(Same clause – proposed enhancement)	Since S.No. 23.7 restricts Bank data storage to the Bank's network, Bank is requested to confirm whether the SMS gateway (which handles employee mobile numbers and responses) must be deployed on-premise within the Bank's network. Bank may consider amending the clause to read: 'The solution shall include its own SMS gateway, deployable on-premise within the Bank's network, capable of sending simulated messages from legitimate mobile numbers, with upload of target numbers, custom message content and scheduled launch date/time.'	The Bank clarifies that the SMS gateway will be provided and managed by the Bank. The proposed phishing/vishing managed service shall integrate with the Bank's SMS gateway for sending simulated phishing/vishing SMS messages to designated employees.
2709	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 19.1 (b), (c)	(b) Developing of look-alike website/portal. (c) Design a webpage to be redirected from the phishing email and to capture the user information/credentials in encrypted form.	Capturing and storing employees' actual credentials – even in encrypted form – creates an avoidable security and DPDP exposure for the Bank (refer 7.6.8 (7) on PII protection). Bank is requested to amend the clause to: 'The landing page shall capture the credential-submission event (user identity and timestamp); the password/secret shall not be stored – only a masked indicator or the fact of submission shall be recorded.' Please also confirm (a) that Bank will authorise registration and use of look-alike domains resembling Bank's brand solely for the simulation and that domain registration is the bidder's responsibility; and (b) that the platform should validate recipient email domains against a Bank-approved domain list before launch to prevent unintended delivery outside the Bank.	No Change, Please be guided by the RFP. The requirement for capturing user interaction/ credential submission during simulation shall be as per the requirement defined in the RFP. However, actual passwords/secrets shall not be retained beyond what is necessary for the authorised simulation and shall be protected in accordance with the Bank's security and data-protection requirements. The Bidder shall propose a secure implementation and obtain Bank approval before campaign execution.
2710	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 19.1 (e)	Testing the servers and filters: Check if the servers and filters are bypassed for simulation.	Bank is requested to confirm whether the Bank will safelist the simulation sending domains / IP addresses at its email security gateway, proxy and endpoint security (the industry-standard approach, so that human behaviour rather than gateway efficacy is measured), or whether the bidder is expected to actively evade the Bank's email security controls. If the former, please share the email security gateway product(s) in use so that safelisting instructions can be provided; if the latter, please confirm that delivery failures caused by Bank's controls will not be treated as bidder non-performance under Section 13.	No Change, Please be guided by the RFP. The Bidder shall coordinate with the Bank for necessary allow-listing/safelist configuration required to conduct authorised simulations. The objective is to assess employee awareness and response to simulated phishing activity. The Bidder shall not undertake unauthorised circumvention of the Bank's security controls.
2711	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 19.2 (f), 19.3 (h)	Executables for Vishing attack / Phishing attack need to be provided by the Bidder.	Bank is requested to clarify the term 'executables'. We understand this to mean the attack artefacts – call scripts/pretexts, simulated payload files (harmless attachments), landing pages and mobile-app packages – and not actual malicious binaries to be executed on Bank endpoints, which would conflict with the Bank's endpoint security policy. Kindly confirm and, if appropriate, amend the wording to 'attack scenarios, scripts and simulation artefacts'.	No Change, Please be guided by the RFP. The term "executables" shall be interpreted as simulation artefacts, attack scenarios, scripts, harmless attachments/payloads and other artefacts required for authorised phishing/Vishing exercises. Actual malicious code shall not be introduced into the Bank environment.
2712	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 19.2 (g), 19.3 (c), 19.3 (i) vs 23.7	Vendor shall arrange Server and other infrastructure for the exercise at their own cost; hosting the phishing mobile application in Vendor's location – versus 23.7: bidder should not store any bank data in vendor location.	S.No. 19.2 (g), 19.3 (c) and 19.3 (i) require the vendor to host vishing and mobile-phishing infrastructure at its own location/cost, whereas S.No. 23.7 states that no Bank data shall be stored at the vendor location for phishing activity. Bank is requested to confirm that: (a) the phishing simulation platform and campaign/user data shall reside as per the deployment model confirmed under 7.2.3 (refer query above); (b) vishing telephony, SMS gateway (if not on-premise) and mobile-app hosting may reside at the vendor's India-based infrastructure with encryption in transit/at rest and purge of PII within a defined period after each exercise; and (c) data residency within India per 7.6.8 (6) is the governing requirement for all components.	a) No Change, Please be guided by the RFP. Bank is seeking the services and hence, bidder is required to factor all requiste component/infrastructure to ensure the delivery of the service. b) Vishing telephony infrastructure and mobile-phishing application hosting may be hosted at the bidder/OEM's India-based infrastructure as part of the proposed off-site managed service. The SMS gateway shall be provided by the Bank. The bidder/OEM shall integrate its proposed solution with the Bank's SMS gateway. All Bank-related data, including employee mobile numbers, campaign data, responses, logs and other PII processed by the bidder/OEM, shall be protected by appropriate encryption in transit and at rest, with access restricted to authorised personnel/processes. The bidder/OEM shall follow the principle of minimum necessary data processing and shall securely purge PII and other Bank data after the Bank-defined retention period, subject to applicable audit, investigation, legal or regulatory retention requirements. c) The bidder/OEM shall not use Bank data for any purpose other than providing the contracted services and shall not use such data for its own analytics, product development, training, benchmarking or any other secondary purpose without the Bank's prior written approval. The bidder/OEM shall remain responsible for the security, confidentiality, integrity, availability and lifecycle management of Bank-related information processed through the service.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2713	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 19.3 (a)	Developing look alike mobile application (Android and iOS) for phishing attack.	Publishing a look-alike banking application on Google Play or the Apple App Store is not permitted under store policies, and iOS does not permit side-loading. Bank is requested to confirm the intended distribution mechanism: (a) Android APK via link/QR code (requires 'unknown sources' to be enabled, normally blocked by Bank MDM); (b) enterprise distribution through Bank's MDM; or (c) a mobile-web / PWA look-alike app experience delivered through smishing or QR code, which works on both Android and iOS without installation. Bank may consider accepting option (c) as compliant for both platforms, or treating the iOS native app as 'desirable'.	No Change, Please be guided by the RFP. The Bidder shall provide the required mobile phishing simulation capability for Android and iOS platforms. The Bidder shall propose a technically feasible and secure delivery mechanism compliant with the applicable platform policies and Bank security requirements.
2714	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 20.1, 20.2	Detailed report … may be required to be presented before Senior Management/Committee; review of results and feedback in a workshop setting.	Bank is requested to specify (a) the number of review workshops and Senior Management/Committee presentations per year; (b) whether they are to be held onsite at the CISO Cell, Rohini, Delhi or virtually; and (c) whether the detailed report is required per campaign or as a consolidated periodic report. Please also confirm that 'user data/credential collected' in the report refers to the list of users who submitted data and not the credential values themselves (refer query on S.No. 19.1 (c)).	No Change, Please be guided by the RFP. The Bidder shall provide detailed reports and presentations/workshops as required by the Bank. The Bank may require the Bidder to present results to Senior Management/Committee during the contract period. Actual credential values shall not be included in reports.
2715	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 20.4, 20.5	Communication to all targeted employees through email for their response … Infographics of key indicators … to be provided within 3 days of completion of exercise.	Bank is requested to confirm whether post-simulation communication to employees is to be (a) delivered automatically by the platform at the moment of click/submission (just-in-time teachable-moment page) and/or (b) sent as a consolidated email after campaign closure from the Bank's official mailbox. Please confirm that '3 days' means three working days from campaign closure and that the infographic may be delivered through the platform/email.	No Change, Please be guided by the RFP. The Bidder shall provide the required employee communication and infographics within 3 days of completion of the exercise, as specified in the RFP. The Bidder shall propose the mechanism for delivery as part of its service.
2716	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 21.1, 21.2, 21.12	Mandatory training modules for phished employees; platform should force the phished employee for completion of training; automated escalation to reporting stakeholders.	To make 'force completion' measurable, Bank may consider amending S.No. 21.2 to read: 'Training shall be auto-assigned to users who fail a simulation; training videos shall not be fast-forwardable; playback shall pause automatically if the training window is minimised or loses focus and resume when re-opened; the percentage of video actually viewed shall be tracked in real time; automated reminders shall be sent for incomplete training, with configurable completion deadlines and escalation to the reporting manager / GRC on breach.' Please also confirm whether Bank has an existing LMS with which integration or SCORM export is required.	No Change, Please be guided by the RFP. Mandatory training shall be assigned to employees identified as having failed the relevant simulation, and completion shall be monitored with appropriate escalation/reporting as specified in the RFP. The Bidder shall provide the required functionality as part of its offiste phishing simulation service.
2717	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 21.7	The platform should include customized learning content such as videos, infographics, posters, wallpapers, gamification, quiz, interactive training content etc.	Bank is requested to indicate the number of training modules expected per year and whether Bank-branded / custom content development is in scope. Bank may also consider specifying the content types more precisely, e.g.: 'story-based short-duration videos depicting real-world cyber-attack incidents with animated characters, cyber-awareness comics, infographics, posters/wallpapers, gamification (points, badges, leaderboards) and quizzes', so that content quality can be evaluated on a uniform basis.	No Change, Please be guided by the RFP. Customised learning content, including videos, infographics, posters, wallpapers, gamification, quizzes and interactive content, is within scope as specified. The Bidder shall provide adequate content to meet the Bank's requirements throughout the contract period.
2718	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 21.5, 21.6, 21.8	Randomize questions and assess users; post-training assessment; certificate on completion.	Bank is requested to confirm (a) the pass threshold and number of attempts permitted for post-training assessments; (b) that random selection of questions from a question bank per user meets S.No. 21.5; and (c) whether certificates are to carry Bank branding/co-branding and be available for download by the employee and export by the administrator.	No Change, Please be guided by the RFP. The platform shall support randomised assessments and post-training assessment/ certificate generation as specified. The Bidder shall demonstrate the proposed assessment/ certification functionality.
2719	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 22.1 – 22.3	Detailed report/dashboard of activities … dashboard for each campaign and access to previous campaigns … customized reports in CSV, Excel and PDF formats.	Bank is requested to confirm whether scheduled/automated emailing of campaign and training reports to designated Bank stakeholders is required, and whether department heads should receive department-level reports automatically. Bank may also consider adding 'campaign-wise email delivery statistics (delivered, bounced, failed) with configurable retry for failed deliveries' to S.No. 22.1, since delivery failures materially affect click-rate interpretation.	The platform shall provide campaign-wise dashboards, historical information and reports in the formats specified in the RFP. The Bidder shall provide required reporting and scheduled dissemination capabilities as part of the proposed solution.
2720	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 22.5	The bidder should provide reports on the latest information security trends and regulatory guidelines … on a frequency mutually agreed with the bank.	Bank is requested to confirm the frequency (monthly/quarterly) and format (advisory note / newsletter) of these reports, and that the requirement is for advisory content on phishing / social-engineering trends and applicable regulatory guidance (RBI, CERT-In, DPDP), and not for a machine-readable threat-intelligence feed (which is separately procured under 7.4.7).	No Change, Please be guided by the RFP. The Bidder shall provide reports/advisories on the latest information-security trends and applicable regulatory guidelines at a frequency defined / adhoc (mutually agreed with the Bank).
2721	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 23.1	The bidder shall perform review of Email solution twice in a year from Cert-IN empaneled organization and compliance verification shall be conducted within 2 months.	Bank is requested to clarify: (a) whether 'Email solution' refers to the phishing simulation platform (i.e., half-yearly VAPT of the platform) or to the Bank's corporate email system; (b) whether the cost of engaging the CERT-In empanelled auditor is to be borne by the bidder; and (c) whether an OEM-arranged periodic VAPT of the platform by a CERT-In empanelled organisation, with closure of findings within two months, will satisfy the requirement.	Please refer addendum for revised clause.
2722	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 23.2	The platform should provide a separate dashboard for monitoring of DMARC/DNS Monitoring for Bank's Email solution.	DMARC/DNS monitoring is a capability distinct from phishing simulation and overlaps with 7.4.5 Anti-Phishing / 7.4.9 Brand Protection. Bank is requested to clarify the scope: (a) number of Bank-owned email domains to be monitored; (b) whether Bank will publish DMARC RUA/RUF records directing aggregate/forensic reports to the solution; (c) whether monitoring covers SPF/DKIM/DMARC alignment only or also look-alike / typo-squat domain detection; and (d) whether this may be delivered as a module within the phishing platform, as a separate tool, or by the Anti-Phishing / Brand Protection service.	Please refer addendum for revised clause.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2723	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 23.3	Support and Update (carries 10 marks in the evaluation sheet).	S.No. 23.3 appears to be a section heading but carries 10 marks in the evaluation sheet. Bank is requested to confirm whether it is a scored item and, if so, what is to be evaluated, or to correct the marking so that the total marks and the 85% threshold are computed correctly.	Please refer addendum for revised clause.
2724	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 23.4 (read with Key Information, p.8)	24*7 support … In case the issue is not resolved for more than 8 hours, support personnel should visit Bank's CISO Office at Mumbai or at Hyderabad.	The RFP Key Information (p.8) locates the Bank's CISO Cell at the Staff Training Centre, Rohini, Delhi, whereas S.No. 23.4 refers to Mumbai or Hyderabad. Bank is requested to confirm the location(s) for onsite support visits. Please also confirm the severity classification to which the 8-hour resolution / onsite-visit condition applies (all issues, or Critical/High only), whether remote resolution with Bank's consent will be accepted, and the applicable penalty framework under Section 13.	Please refer addendum for revised clause.
2725	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 23.5, 23.6	Updation of new features and upgradation of on-premise platform automatically from time-to-time; updates/upgrades free of cost during contract period.	If an on-premise deployment is confirmed under 7.2.3, Bank is requested to confirm: (a) whether the platform will be permitted outbound internet/proxy access for automatic updates, or whether updates are to be applied through offline packages under Bank's change-management process; (b) whether Bank will provide the compute (VM / CPU / RAM / storage at DC and DR), OS and database licences, or the bidder is to supply hardware/appliances and include a non-production environment per Annexure 21; and (c) that Bank will provide an SMTP relay / outbound mail path and DNS entries for the simulation domains.	No Change, Please be guided by the RFP. The Bidder shall provide updates/upgrades of the proposed platform throughout the contract period at no additional cost. The Bidder shall propose the required deployment/update mechanism in accordance with the Bank's security and change-management policies.
2726	Appx 1C (Excel)	Appendix 1C – Functional Compliance Sheet (Services), Sheet: Phishing Simulation	S.No. 23.7, 23.8	Data storage restricted to Bank network; data at rest and in motion encrypted; adequate security for PII during smishing/vishing.	Bank is requested to confirm the encryption standards to be complied with (e.g., AES-256 at rest, TLS 1.2 or above in transit), whether integration with Bank's HSM/KMS is required, the retention period for campaign and user data (e.g., contract tenure plus a defined period, as Annexure 21 does not specify retention for this service), and the data purge/return requirement at contract exit. Please also confirm that campaign artefacts hosted at the vendor's facility for vishing/smishing/mobile exercises shall be purged within a defined period (e.g., 30 days) after each exercise.	Data at rest and in transit shall be encrypted and appropriate security measures shall be implemented for protection of Bank data/PII. The Bidder shall comply with the Bank's applicable information-security, data-retention, data-purge and data-protection requirements.
2727	—	General – Bank dependencies	Authorisation and pre-requisites for simulated attacks (not specified in 7.4.4 / Appendix 1C)	Written authorisation, HR/Legal sign-off, safelisting, DNS/domain approvals and nodal officer.	Bank is requested to confirm that it will provide, prior to the first campaign: (a) a written authorisation for simulated phishing, vishing, smishing, quishing and mobile-phishing exercises against employees; (b) HR/Legal sign-off and the internal communication policy (whether employees are to be informed in advance that simulations may occur); (c) safelisting at email gateway / proxy / endpoint; (d) DNS / domain approvals; and (e) a nodal officer / SPOC from the CISO Cell.	No Change, Please be guided by the RFP. The Bank shall provide the necessary authorisations, approvals and coordination required for conducting the approved phishing, vishing, smishing, quishing and mobile-phishing simulation campaigns. The specific prerequisites, including HR/Legal approvals, internal communication requirements, safelisting, DNS/domain approvals and designated SPOC, shall be coordinated with the successful bidder as per the Bank's applicable policies and campaign plan prior to commencement of the respective campaign.
2728		Appendix 1A Functional Compliance Sheet (Solutions) CTEM	8	The solution should allow messaging and collaboration within the context of a specific intelligence item	We understand that this scope is for the bidder to collaborate on incidents/alerts within the team.	Please refer the below clarification: Example: CVE is found in multiple endpoints/devices then it should be contextualized and integrate with SIEM for Incident creation The System should provide access to relevant team and share RBAC intelligence
2729			24	The solution should provide pre-built bidirectional integrations with SIEM, SOAR, ticketing (Manage Engine), and threat intelligence platforms	We understand that the bidder will share the data with various on-premises tools like SIEM, SOAR, and ticketing tools (ManageEngine); hope this meets your requirement.	Please refer addendum for revised clause
2730			31	The solution should display a Security Score overview with full breakdown by issue category	Can the bidder provide the risk rating of the organization? We hope this will suffice the requirement.	Yes, Solution Need to provide Risk Rating on the Infrastructure.
2731			CTEM item 35	The solution should detect malicious files, reconnaissance activity, automated attack tools, and target lists	We understand that the bidder can achieve this functional requirement using a combination of tools like SIEM, SOAR, and other SOC components.	Please refer addendum for revised clause
2732			43	The ML model should continuously study the environment including asset relationships, topology, and security controls to detect false positives and identify root causes	We understand that the bidder can achieve this functional requirement using a combination of tools like SIEM, SOAR, UEBA, and other SOC components like TIP or EDR.	Yes, Understanding is correct
2733			48	The solution should assess and harden network, endpoint, and operating system security controls	We understand that the bidder can achieve this functional requirement using a combination of tools like SIEM, SOAR, UEBA, and other SOC components like TIP or EDR, including the day-to-day operations of SOC analysts.	Please refer addendum for the revised clause
2734			51	The solution should apply virtual patching/compensating controls/exposure mitigation mechaism to the firewall and other security systems through integration with relevant security controls.	We understand that the bidder can take preventive measures on other solutions, either manually or automatically using SOAR, based on the findings received from the CTEM solution.	Please refer addendum for the revised clause
2735			62	The solution should leverage compensating controls and layered defense strategies to manage threats proactively	We understand that this requirement can be achieved by the bidder through analysts managing the SOC during their day-to-day operations.	Please refer addendum for revised clause
2736		Appendix 1A Functional Compliance Sheet (Services) ASM	3	Solution should store historical information about bank to provide cybersecurity maturity over time	We understand that bank requires solution to store a detailed/ historical information on the detections and the attacks which were targeted on during the complete contract duration.	Yes, Your understanding is correct
2737			24	The solution must allow the organization to define the prioritization of assets based upon impact of the asset	We undestand that bank requires special attention/priortization to specific assests, so the bank can take preventive measures/ obseravility on it, it may be like assigning tags to certain important tags and creating a dashboard for critical ones.	Yes, your understanding is correct
2738			26	Solution must provide a workflow to define and manage state of discovered entities which affects the priority of the entity.	We understand that bank requires the solution to enable workflow for alerting the adminsitrators for any vulnerability detection on the discovered critical assests.	Yes, your understanding is correct

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2739			35	Solution should have the feature to automatically create help desk ticket containing asset meta data, comments, link back to the solution console and guidance. Ticket status should be automatically reflected in ASM console.	Please amend the clause as: Solution should have the feature to automatically create help desk ticket containing asset meta data, comments, link back to the solution console and guidance. Justification: We want authorities to clarify this, as we understand that bank requires ASM console to create tickets automatically for the detections and analysts to work upon?	Please refer addendum for the revised clause
2740			38	Solution must have bi-directional, writetable API's that allow the organization to integrate data into the organization's existing security	Please amend the clause as: Solution must have API's that allow the organization to integrate data into the organization's existing security Justification: since its services scope which is used to provide the outside attack surface details not the TIP Functionality so bidirectional API are not part of it.	Please refer addendum for the revised clause
2741		Appendix 1A Functional Compliance Sheet (Services) Brand Abuse	25	The Bidder should provide for identification of fake recruitment schemes claiming affiliation with the Bank	We understand that bank requires solution to provide for identification of fake recruitment schemes claiming affiliation with the Bank which has the bank names and logo or any other identification method	Please refer addendum for revised clause
2742			33	Search engines (like Google, yahoo, bing etc.) listing frauds where the customer care number & branch address of banks is changed/ modified should be continuously tracked and the same should be brought down immediately including True caller and JustDial.	Please delete this cluase its oem specific. Please modify the clause as to make it vendor neutral: Monitoring all major mobile app marketplaces for counterfeit, copycat apps, or apps infringing trademarks	Please refer addendum for the revised clause
2743			37	Bidder should be able to identify and report to the bank if access to blocked ports on a webserver is sought by an external user.	We understand that the ask is not resticted to Brand abuse solution bidder can achive this requirenment with the combination of multiple solutions as it would also requires logs from perimeter and application security solutions, its is part of SIEM Solution.	Please refer addendum for the revised clause
2744		Appendix 1A Functional Compliance Sheet (Services) Dark Web Monitoring	21	Monitor suspicious SSL/TLS certificate issuance.	We understand that bidder can achive this requirenement from either services product like ASM, Brand abuse or TI, this ask is not restrcited to DWM. As functional requirenment of bank is achieved anyways.	Yes, Understanding is correct
2745			25	Provide Passive DNS intelligence and historical DNS resolution.	We understand that bank requires DNS intelligence and bank wants the bidder to store the historical logs/analysis of the DNS specific abuse.	Yes, your understanding is correct
2746			40	Monitor C2 infrastructure, malware hosting, phishing infrastructure and botnets.	We undertand that bank requires information about the fake webistes which impersonating as PSB to Monitor C2 infrastructure, malware hosting and phishing infrastructure and botnets.	Yes, your understanding is correct
2747			44	Support Email, SMS, and other notifications based on configurable severity.	We understand that bidder can achive this requirenment by combination of multiple products to achive this functionality spcifically ITSM.	Yes, your understanding is correct
2748				clarifications	Please clarify: Does the solution have an established threat intelligence capability with more than 8 years of experience in global threat intelligence collection, analysis and threat actor tracking?	No Change, Please be guided by the RFP
2749				clarifications	Please clarify: Does the solution leverage intelligence from a global network of 400+ threat researchers, analysts and threat hunters?	No Change, Please be guided by the RFP
2750				clarifications	Please clarify: Does the solution collect and analyze threat intelligence across 14+ languages and sources?	No Change, Please be guided by the RFP
2751				clarifications	Please clarify: Does the solution provide threat intelligence derived not only from network and publicly available sources, but also from active monitoring, engagement and communication with relevant threat actor groups and underground communities to identify planned attacks, emerging campaigns, TTPs, compromised assets and indicators of compromise?	No Change, Please be guided by the RFP
2752				clarifications	Please clarify: Does the solution provide actionable threat intelligence on threat actor groups and campaigns, including their objectives, targeting, attack methods, TTPs, infrastructure and intended victims, along with recommended mitigation and protection measures to help the organization proactively defend against such threats?	No Change, Please be guided by the RFP
2753		Appendix 1A Functional Compliance Sheet (Services) Threat Hunting	3	Create use-cases correlation rules specific to client's environment and event sources.	We understand that the bidder can achieve this functional requirement using a combination of tools like SIEM, SOAR, UEBA, and other SOC components like TIP or EDR, including the day-to-day operations of SOC analysts. OEM, Services do not directly perform detection engineering. We however provide recommendations on identified gaps in detections	No Change, Please be guided by the RFP
2754			9	Review effectiveness of SOC to detect similar events..		No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2755			13	Threat Hunting shall also address the following If the SOC has detected the attack, then identify the reasons for no action being taken if the SOC has not detected the attack, then identify if an existing correlation rule requires tuning or if a new correlation rule is required or if a new solution is required.		No Change, Please be guided by the RFP
2756				clarifications	Since RFP Ask for the Threat hunting servcies from OEM but does not define the no of hours: Please clarify that the solution should be sized on the below: Vendor shall propose a 200-hour package to start with along with per hour cost and Bank shall decide to extend the number of hours depending on scope expected	No Change, Please be guided by the RFP Refer Section 7.2.2 Services
2757				clarifications	Please clarify: Does the proposed service provide organization-wide ransomware readiness and threat hunting across the complete security ecosystem, including infrastructure/products, people and processes, to proactively identify ransomware-related risks, vulnerabilities, attack paths, indicators and gaps, along with recommended remediation actions?	No Change, Please be guided by the RFP. The requirement shall be interpreted in accordance with the scope and functionalities specified under Section 7.4.8 – Threat Hunting Services, Appendix 1C. The Threat Hunting Service is intended to provide proactive, hypothesis-driven and intelligence-led technical threat hunting across the Bank's IT and security ecosystem. The service may utilize relevant telemetry and logs available through the Bank's SIEM, as well as other applicable security technologies and data sources, for identifying known and unknown threats,
2758				clarifications	Please clarify: Does the proposed service provide a comprehensive maturity assessment with a defined maturity rating and actionable recommendations to strengthen the overall cybersecurity program, prioritize security initiatives and investments, and improve business continuity, resilience and recoverability during unexpected cyber incidents?	No Change, Please be guided by the RFP
2759				clarifications	Please clarify: Does the proposed service provide a modular cybersecurity assessment and incident-readiness package offering, at a minimum, the following capabilities as per organizational requirements: SOC Gap Assessment, Ransomware Assessment, Forensic Analysis, Compromise Assessment, Incident Response Readiness Assessment, Active Directory Security Assessment, Tabletop Exercises, and Incident Response Playbook Development?	No Change, Please be guided by the RFP
2760		Appendix 1A Functional Compliance Sheet decoy	20	Includes an algorithm for automated rule creation that integrates with SOAR platforms, enabling real-time blocking of attacker IPs based on threat intelligence gathered from decoys. Features a customizable Generative AI model to assist security analysts with contextual insights, investigative support, and proactive security measures.	Please amend the clause as: Includes an algorithm for automated rule creation that integrates with SOAR platforms, enabling real-time blocking of attacker IPs based on threat intelligence gathered from decoys. Justification: GenAI is a functaionlity of soar solution where SOAR can create and run the playbook as per the event or alert where decoy is reponibsle for redirecting the attacker to fake vm to monitor the actvitites.	Please refer addendum for revised clause
2761			25	The proposed solution shall be delivered as a cloud-based/SaaS platform hosted within the CSP environment. The bidder shall provision and size the required cloud compute, storage, network, and other platform resources to meet the Bank's performance, scalability, High Availability (HA), service continuity, and Disaster Recovery (DR) requirements in accordance with the applicable Cloud Deployment Model.	Please amend the clause as: Proposed Solution must cover complete scope of min of 200 applications, networks, devices with 50 segments across DC-DR and capability to add additional decoy connector through decoy customization as per requirement Justification: Request to amend the requirement to allow an on-premises Deception Solution instead of a cloud-based solution, as cloud-based redirection of decoy traffic may introduce latency and dependency on WAN/Internet connectivity, impacting real-time attacker engagement and the overall effectiveness of deception.	Please refer addendum for revised claus
2762	30	RFP - 7.2 Solution & Services Deployment Model and Their HA Requirement 7.2.1 Solutions – Master Deployment Matrix	6. Network Detection & Response (NDR)	Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Management Console: Deployed at both DC and DR	Different NDR solution works on different redundancy deployment methodology (I.e Active - Active or Active - Passive). Request bank to modify the clause as: Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active/Passive at DC and HA, N+N, Active-Active/Passive at DR. Management Console: Deployed at both DC and DR	Please refer addendum for revised clause
2763	45	RFP - Scope of Work 7.3.5 Network detection and response (NDR)	7.3.5.1 Modules, Architecture & Deployment:	Pt 2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Generally NDR solutions are deployed with sole purpose of doing network analysis, threat detection & response and does not have native 2FA capability, so request bank to remove this point. As an alternate as proposed in same point, proposed NDR solution can be integrated with bank's existing MFA solution.	Please refer addendum for the revised clause
2764	49	RFP - Scope of Work 7.3.10 Application security testing Tool	7.3.10.1 Modules, Architecture & Deployment:	Pt 2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Generally AST solutions are deployed with sole purpose of scanning the source code, web, api etc and does not have native 2FA capability, so request bank to remove this point. As an alternate as proposed in same point, proposed AST solution can be integrated with bank's existing MFA solution.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2765	110	RFP - 10.2 Eligibility Evaluation Criteria	OEM Evaluation Criteria	Pt 19. The proposed OEM SIEM Solution with a minimum capacity of 30,000 EPS or 1.2 TB/day shall have been successfully implemented on cloud in one (1) in India.	For wider participation, we request bank to amend the clause as: The proposed OEM SIEM Solution with a minimum capacity of 5,000 EPS or.2 TB/day shall have been successfully implemented on cloud in any one (1) Govt/PSU customer in India. OR The proposed OEM SIEM Solution with a minimum capacity of 10,000 EPS or.4 TB/day shall have been successfully implemented on cloud in one (1) in India.	Please refer addendum for revised clause.
2766	112	RFP - 10.2 Eligibility Evaluation Criteria	OEM Evaluation Criteria	Pt 20. The proposed OEM solution should have been implemented in at least one BFSI is to be submitted for the following solutions: NDR	For wider participation, we request bank to amend the clause as: The proposed OEM solution should have been implemented in at least one BFSI / Govt is to be submitted for the following solutions: NDR	Please refer addendum for the revised clause
2767	40	APPENDIX 1A Functional Compliance Sheet (Solutions)	Network Detection & Response (NDR)	Pt 13. The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	As bank has asked for on-premise solution for NDR, on the contrary, this clause asks for cloud-native SAAS ask. So, we kindly request bank to delete this clause.	Please refer Addendum for revised clause
2768		NDR Functional Compliance Sheet	Clause 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high- availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	The Clause mandates Cloud based SaaS model, while RFP Page 30, Page 35, section 7.2.4.1 clause 'd' asks for on Premesis solution "The NDR shall be deployed On-Premises". We request to modify the clause to include On-Prem solution. Justification: To include solutions which are on-Prem based	Please refer Addendum for revised clause
2769	Appendix 1A Page 40	NDR Functional Compliance Sheet	Clause 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high- availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	The Clause asks for Active-Active HA architecture, we request to include Active-Standby Mode. Justification: Management Console is central console, it cannot be deployed in Active-Active mode, as it is a central component.	Please refer Addendum for revised clause
2770	Appendix 1A Page 41	NDR Functional Compliance Sheet	Clause 18	Solution should have the capabilities to create and run security playbooks for automation and better MTTD/MTTR on the basis of criticality of threat/server	Proposed solution adopts below appraoch for automated MTTD, Solution need investigative workflows and all the alerts need to be validated before building any Active Response Solution is having inbuilt playbooks like Host, Session and Packet analysis. once alert is validated Active Response can be triggered. Hope the approach is acceptable	Yes, your understanding is correct Also, Please refer addendum for the revised clause
2771	Page 66	7.6.7	Training	At a minimum, the following training programs shall be conducted for each proposed solution / OEM appointed officials: Duration per Session and Munimum Number of Sessions	Overall there is a requirement of 15 Sessions and Duration per session is 2 or 3 days. This takes the total training per solution to 40 days. This is very large reqirement of training, we request to make it to 3 days for NDR solution	Please refer addendum for revised clause
2772	Page 63	7.6.6	Testing, clause 3	The bidder shall provision and maintain dedicated Development, Testing, UAT, and Pre-Production environments throughout the contract period.	Is UAT Environment required for NDR solution also, given that NDR is a Passive and out of path solution.	Please refer addendum for revised clause
2773		ITDR	1.7	Detect and respond to active threats with high fidelity (low false positives and false negatives).	Pre-Bid Query / Clarification: The Bank has separately specified a comprehensive deception platform for detection of active attacker activity, reconnaissance and lateral movement. We understand that the intent of this clause within ITDR is therefore to complement those controls with focused monitoring of the Bank's most critical identities. Considering that enhanced user-activity monitoring is most relevant for high-risk personnel such as executives, privileged users and other critical users, we request the Bank to kindly clarify whether this requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should provide high-fidelity detection and response for risky or anomalous user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, to identify activities associated with careless, malicious or compromised users.	No Change, Please be guided by the RFP
2774		ITDR	1.8	Provide contextual information—who, what, when and how—to inform all stages of the attack chain.	Pre-Bid Query / Clarification: The Bank has already sought attack-lifecycle visibility under the separate deception requirements. For ITDR, we understand that additional value would be derived from detailed user-centric context for the Bank's most critical identities, enabling investigation of risky activity performed by such users. We request the Bank to kindly clarify whether this requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should provide contextual information—who, what, when, where and how—around risky user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, to support investigation and response.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2775		ITDR	1.9	Provide deep insights into both the potential and used privilege escalation and lateral movement steps in an attack.	Pre-Bid Query / Clarification: Privilege escalation and lateral-movement visibility is already substantially addressed under the separately specified deception solution, including attacker lifecycle visibility, MITRE ATT&CK mapping, deceptive attack paths and detection of lateral movement. To avoid duplication while retaining complementary investigation capability for high-risk identities, we request the Bank to kindly clarify whether this requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should provide deep insights into activities performed by up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, covering application usage, file and data movement, endpoint activity and other risky behaviours to support investigation of compromised, malicious or negligent user activity.	No Change, Please be guided by the RFP
2776		ITDR	2.9	Detect all types of attack vectors including pre-attack reconnaissance, zero-day attacks, privilege escalation prevention, lateral movement and data theft.	Pre-Bid Query / Clarification: Pre-attack reconnaissance, lateral movement, malware/attack behaviour and attacker lifecycle visibility are already covered under the Bank's separate deception specifications. We understand that the complementary requirement under ITDR should focus on identity/user risk and potential data-loss activity for the Bank's most critical users rather than duplicate the deception control. We request the Bank to kindly clarify whether this requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should detect risky user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, including suspicious application usage, unauthorized access or movement of sensitive information, removable-media activity, web-based transfer, cloud synchronization and other potential data-exfiltration activities.	The Clause is applicable only to idendity related threat vector only. The volumetrics is provided in the RFP and should be complied
2777		ITDR	2.10	Detect multiple attacks simultaneously.	Pre-Bid Query / Clarification: We understand the intent is to ensure that the solution is not restricted to investigation of a single event at a time. Since active attacker detection is separately covered by the deception solution, we request that this clause be clarified in terms of concurrent monitoring and investigation of risky activities across the Bank's designated critical-user population: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should be capable of detecting and investigating multiple risky user and data activities simultaneously across up to 100 critical/high-risk users and their monitored endpoints.	No Change, Please be guided by the RFP
2778		ITDR	3.2	Provide unified presentation of both source- and target-based telemetry data in a timeline view.	Pre-Bid Query / Clarification: The Bank has separately specified end-to-end attacker visibility and behavioural analysis under the deception solution. For ITDR investigations involving critical identities, a chronological user-activity view would provide complementary evidence of actions performed by the user. We request the Bank to kindly clarify whether the requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should provide a unified chronological timeline of user- and endpoint-based activity telemetry for up to 100 critical/high-risk users identified by the Bank to support investigation of risky or suspicious user activity.	No Change, Please be guided by the RFP
2779		ITDR	3.3	Correlate identity-related telemetry from relevant source and target systems to identify and investigate identity compromise, privilege escalation, credential abuse and lateral movement.	Pre-Bid Query / Clarification: Privilege escalation and lateral-movement detection are already addressed through the separately specified deception controls. To provide complementary investigation capability for the Bank's highest-risk identities, we request the Bank to clarify whether this clause may focus on correlation of user, endpoint, application and data activity for the designated critical-user population: Suggested Clarified Wording / Requested Action: The solution shall support correlation of user, endpoint, application and data-activity telemetry for up to 100 critical/high-risk users identified by the Bank to identify and investigate suspicious user behaviour, sensitive-data movement, policy violations and potential data-exfiltration activities.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2780		ITDR	3.4	Integrate with compatible endpoint/extended detection solution to capture screen recordings or screenshots during active attacker sessions as advanced forensic evidence.	Pre-Bid Query / Clarification: The Bank has separately specified attacker-session and forensic visibility through the deception platform. Within ITDR, we understand that visual evidence is intended to strengthen investigation of high-risk user activity. We request the Bank to kindly clarify whether the requirement may be read in an outcome-based manner for the designated critical-user population: Suggested Clarified Wording / Requested Action: The Identity Threat Detection Solution should support screenshots, screen capture or equivalent visual evidence of relevant activity for up to 100 critical/high-risk users during suspicious or high-risk user sessions, as part of forensic investigation and evidence collection.	Please refer addendum for revised clause
2781		ITDR	3.5	Integrate with compatible network detection solution to support collection of PCAP data for network-level incident visibility.	Pre-Bid Query / Clarification: The requirement for PCAP is network-centric and does not directly relate to identity posture or focused user-activity monitoring. Further, the Bank's separate deception specifications already require high-interaction decoys, recording of attacker activities, traffic/behaviour visibility, forensic investigation and integration with network/security technologies. To avoid duplication of network-level forensic controls across two solution categories, we request the Bank to kindly delete this clause from the ITDR section. Suggested Clarified Wording / Requested Action: Requested action: Delete Clause 3.5 from the ITDR requirements, as equivalent/complementary network and attacker forensic visibility is already sought under the separate Deception requirements.	Please refer addendum for revised clause
2782		ITDR	3.6	Push incident data into SIEM/XDR or SOAR technologies via integrations for improved incident management.	Pre-Bid Query / Clarification: We understand that the objective is to ensure relevant ITDR alerts and investigation context are available to the Bank's SOC ecosystem. For the enhanced monitoring of designated critical users, we request the Bank to kindly clarify whether alerts and activity information may be shared through supported integrations or APIs as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should make alerts and relevant incident/activity data for the monitored critical-user population available to SIEM/XDR, SOAR or other supported security platforms through integrations or APIs for improved incident management.	The proposed solution hould be integrated with SIEM/XDR or SOAR technologies for sharing the incident data via supported integrattion or APIs
2783		ITDR	3.7	As part of forensic data collection, include detailed attack path information including protocols leveraged during the attack.	Pre-Bid Query / Clarification: Detailed attack-path and attacker-behaviour visibility is already sought under the separate deception specifications, including deceptive attack paths, MITRE ATT&CK mapping and forensic investigation. To avoid overlap while retaining complementary evidence for investigations involving the Bank's critical identities, we request the Bank to kindly clarify whether the requirement may be read as follows: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should, as part of forensic data collection for up to 100 critical/high-risk users, include detailed user-activity information such as applications used, files accessed, data movement, destination channels and other relevant endpoint activity associated with the incident.	Please refer addendum for revised clause
2784		ITDR	3.8	Collect user and computer information from Active Directory as part of forensic data gathering to enhance context and assess risk exposure.	Pre-Bid Query / Clarification: We understand that directory information is required to enrich investigations with user and computer context. We request the Bank to clarify that enterprise identity context may be maintained for the overall identity population, while detailed endpoint/user-activity telemetry may be applied to the Bank's designated critical-user population: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should use relevant user and computer identity information to enhance forensic context and risk assessment, and should correlate such context with detailed endpoint/user-activity telemetry for up to 100 critical/high-risk users identified by the Bank.	Please refer addendum for revised clause
2785		ITDR	3.9	Detect an adversary's attempt to move laterally toward key assets using as many Windows, Mac or Linux hosts as possible without requiring a persistent agent.	Pre-Bid Query / Clarification: The Bank's separate deception specifications expressly require detection of lateral movement, reconnaissance, credential theft and malicious activity using agentless and/or agent-based deception techniques across the enterprise. The present clause therefore duplicates a capability already being procured under the Deception section. To avoid overlapping scope and duplicate controls, we request the Bank to kindly delete this clause from the ITDR section. Suggested Clarified Wording / Requested Action: Requested action: Delete Clause 3.9 from the ITDR requirements, since lateral-movement detection using deception techniques is already explicitly covered under the separate Deception specifications.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2786		ITDR	3.10	Collect AD user/computer information for forensic context and detect at the earliest point post initial compromise as the attacker first attempts lateral movement and privilege escalation.	Pre-Bid Query / Clarification: Early detection of lateral movement and privilege-escalation activity is substantially covered under the Bank's separate deception requirements. To retain a complementary identity/user-risk objective without duplicating the deception scope, we request the Bank to kindly clarify whether this clause may focus on early detection of risky activity among the designated critical-user population: Suggested Clarified Wording / Requested Action: Identity Threat Detection Solution should use relevant identity context and detect risky user behaviour at the earliest possible point for up to 100 critical/high-risk users, based on monitored endpoint activities and configured detection policies, enabling investigation and response before such activity results in significant data loss or business impact.	Please refer addendum for revised clause
2787		ITDR	3.11	Collect AD user/computer data during forensic gathering while ensuring all deception techniques remain hidden from legitimate users.	Pre-Bid Query / Clarification: The requirement to ensure deception techniques remain hidden from legitimate users is inherently a deception-platform capability. The Bank has already included comprehensive deception requirements covering lures, breadcrumbs, fake credentials, deceptive assets, attacker engagement and techniques designed to remain undetected by attackers. We therefore request the Bank to kindly delete this clause from the ITDR section to avoid duplication. Suggested Clarified Wording / Requested Action: Requested action: Delete Clause 3.11 from the ITDR requirements, as deception techniques and their concealment are already covered under the separate Deception specifications.	Please refer addendum for revised clause
2788		Anti Phishing	17.1	Solution should detect at the earliest point in the attack, post initial compromise as the attacker is first attempting to move laterally and escalate privilege.	Pre-Bid Query / Clarification: Since this section is focused on Anti-Phishing, we understand that the objective is to identify suspicious activity following a successful phishing or account-compromise event. Network-level lateral movement and deception capabilities may be addressed by other security controls. We request the Bank to clarify whether this clause may instead focus on early post-compromise user activity visibility for the Bank's most critical users. Suggested Clarified Wording / Requested Action: The solution should support early identification and investigation of suspicious user activities associated with potential account compromise following phishing or other email-originated attacks, with enhanced user activity monitoring for up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles.	Please refer to the relevant Addendum for updated specfications
2789		Anti Phishing	17.4	Solution must provide robust supply chain and AI/ML-driven contact chain analysis capabilities to identify and defend against socially engineered, impersonated, or BEC attacks.	Pre-Bid Query / Clarification: As compromise of trusted suppliers and partners is an important source of BEC and phishing risk, we request the Bank to clarify whether the existing supply-chain requirement should explicitly include behavioural analysis of supplier/partner communication patterns to identify attacks originating from compromised trusted accounts. Suggested Clarified Wording / Requested Action: Solution must provide robust supply-chain and AI/ML-driven contact-chain and behavioural analysis capabilities to identify and defend against socially engineered, impersonated or BEC attacks, including threats originating from compromised or impersonated supplier/partner accounts.	Please refer to the relevant Addendum for updated specfications
2790		Anti Phishing	18	Solution must proactively analyze suspicious URLs using dynamic/behavioral analysis to prevent the spread of malware and other threats.	Pre-Bid Query / Clarification: The RFP separately addresses URL analysis and post-delivery remediation. We request clarification whether these requirements are intended to provide continuous protection throughout the email threat lifecycle, including pre-delivery analysis, click-time URL protection and post-delivery detection/remediation. Suggested Clarified Wording / Requested Action: Solution must provide continuous protection across the email threat lifecycle, including pre-delivery threat detection, real-time/click-time inspection of suspicious URLs, and post-delivery detection and automated remediation of threats that are subsequently determined to be malicious.	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2791		Anti Phishing	19.7	Solution must be able to offer a comprehensive portal that allows users to access information and metadata on events/incidents, facilitating network threat forensics for thorough investigation and analysis of potential security breaches or incidents.	Pre-Bid Query / Clarification: To strengthen investigation of phishing-led incidents involving executives and other critical users, we request clarification whether the existing forensic portal requirement may also include contextual user and endpoint activity for a limited population of Bank-identified critical/high-risk users. Suggested Clarified Wording / Requested Action: Solution must offer a comprehensive investigation portal providing information and metadata on events/incidents for forensic analysis. For up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, the portal should additionally provide contextual user and endpoint activity, including relevant application, file and user-action details, to support investigation of potential phishing-led compromise.	Please refer to the relevant Addendum for updated specfications
2792		Anti Phishing	19.9	Solution must empower security operations and incident responders to automate the identification, remediation, and sharing of phishing threats, streamlining the process of detecting, addressing, and disseminating information about potential phishing attacks for improved response and mitigation.	Pre-Bid Query / Clarification: To improve SOC investigation efficiency, we request clarification whether the existing phishing identification and remediation requirement should include centralized attack context showing why a message was identified as malicious, the users targeted, associated threat indicators and remediation status. Suggested Clarified Wording / Requested Action: Solution must empower security operations and incident responders to automate identification, investigation, remediation and sharing of phishing threats, and should provide centralized contextual visibility into the users targeted, associated threat indicators, detection rationale, attack characteristics and remediation actions.	Please refer to the relevant Addendum for updated specfications
2793		Anti Phishing	19.1	Solution must provide incident responders with real-time analytics and visibility into email-based attacks targeting the organization.	Pre-Bid Query / Clarification: Email-based attacks against executives and privileged users may require additional context after delivery to determine whether a targeted user has subsequently performed suspicious activity. We request the Bank to clarify whether real-time investigation visibility may include relevant user activity context for up to 100 Bank-identified critical/high-risk users. Suggested Clarified Wording / Requested Action: Solution must provide incident responders with real-time analytics and visibility into email-based attacks targeting the organization. For up to 100 Bank-identified critical/high-risk users, the solution should additionally provide contextual visibility into suspicious user activities associated with potential phishing or account compromise, including relevant user, endpoint, application and file activity.	Please refer to the relevant Addendum for updated specfications
2794		Anti Phishing	19.23	Solution must have simplicity of evaluation and additional visibility into internal traffic and other communication channels can reduce risk, and baseline user activity to detect suspicious behavior.	Pre-Bid Query / Clarification: The existing clause already seeks baselining of user activity to detect suspicious behaviour. We request the Bank to clarify the intended depth and scope of this capability and whether enhanced monitoring may be applied to a focused population of up to 100 Bank-identified critical/high-risk users, where deeper visibility provides the greatest security value. Suggested Clarified Wording / Requested Action: Solution must provide additional visibility into relevant internal activity and communication channels to reduce risk and baseline user activity to detect suspicious behaviour. Enhanced user and data activity monitoring should be provided for up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, with configurable detection policies for suspicious, anomalous or policy-violating activities.	Please refer to the relevant Addendum for updated specfications
2795		Anti Phishing	19.7	Solution must provide protection against harassment mail and mitigate the risks associated with emails from unknown senders specifically for executives or VIPs, safeguarding them from potential threats and ensuring their email communication remains secure.	Pre-Bid Query / Clarification: Since this clause already provides enhanced protection for executives/VIPs, we request the Bank to clarify whether such enhanced protection should extend beyond receipt of suspicious email to investigation of risky user and data activities that may occur following phishing or account compromise, for a limited set of the Bank's most critical users. Suggested Clarified Wording / Requested Action: Solution must provide protection against harassment mail and mitigate risks associated with emails from unknown senders specifically for executives or VIPs. For up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, the solution should additionally provide enhanced visibility into risky user and data activities following suspected phishing or account compromise, including relevant file movement, web/upload activity, removable-media activity and other supported data-transfer channels.	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2796		Cloud	1	OEM shall ensure compliance of the complete proposed solution & platform with RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and all applicable regulations throughout the contract period.	Pre-Bid Query / Clarification: We request the Bank to clarify that the OEM is required to maintain applicable security, privacy and regulatory controls relevant to the services provided and furnish available compliance/assurance documentation, while the overall regulatory compliance obligation of the Bank remains subject to the Bank's deployment, configuration and usage of the service. Suggested Clarified Wording / Requested Action: OEM shall maintain security, privacy and compliance controls applicable to the proposed hosted service and shall provide available independent assurance reports, certifications and relevant compliance documentation to support the Bank's obligations under applicable RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and other applicable regulatory requirements.	Please refer addendum for revised clause
2797		Cloud	2	The Service uptime agreement for the proposed solution on cloud should have monthly uptime commitments and have transparent monthly credit calculations in case of uptime not being met for any services.	Pre-Bid Query / Clarification: We understand that published/contracted OEM hosted-service SLA commitments and corresponding service-credit methodology shall meet this requirement. Kindly confirm. Suggested Clarified Wording / Requested Action: Retain clause, with clarification that the applicable OEM hosted-service SLA and service-credit schedule will govern the commitment.	No Change, Please be guided by the RFP
2798		Cloud	3	Solution provider should provide the design and process for data deletion in the scope of an independent audit and that the operational effectiveness of these controls is tested. The report for the same should be submitted to bank as and when asked by bank.	Pre-Bid Query / Clarification: For a globally operated hosted security service, control effectiveness is generally evidenced through independent assurance reports such as SOC 2 Type II and documented data-retention/deletion controls. We request the Bank to permit such independent assurance documentation instead of requiring a separate bespoke data-deletion audit report. Suggested Clarified Wording / Requested Action: Solution provider shall maintain documented secure data-retention and deletion controls. Compliance may be demonstrated through applicable independent third-party assurance reports/certifications (such as SOC 2 Type II or equivalent) and documented data-retention/deletion policies made available subject to OEM confidentiality requirements.	Please refer addendum for the revised clause
2799		Cloud	4	Independent audit for testing effectiveness of secure data removal, such that data is rendered permanently inaccessible. (Including any backup or distributed online media).	Pre-Bid Query / Clarification: We request the Bank to accept independently audited secure deletion and media-management controls, together with documented retention/deletion periods, rather than requiring a customer-specific audit of all backup and distributed media. Suggested Clarified Wording / Requested Action: The OEM shall maintain secure data deletion, media handling and backup-retention controls designed to render customer data inaccessible in accordance with documented retention schedules. Effectiveness may be evidenced through independent assurance reports such as SOC 2 Type II/ISO 27001 or equivalent and relevant OEM security/privacy documentation.	Please refer addendum for the revised clause
2800		Cloud	5	Bank shall have an option to implement 'Bring Your Own Key' as and when required.	Pre-Bid Query / Clarification: The proposed service protects data at rest and in transit using strong encryption; however, customer-managed infrastructure encryption keys are not a standard capability of the hosted anti phishing service. We request deletion of the BYOK requirement, or acceptance of OEM-managed enterprise-grade encryption and key-management controls. Suggested Clarified Wording / Requested Action: Requested Action: Delete the BYOK requirement. Alternatively: 'Data processed/stored by the hosted service shall be protected using industry-standard encryption in transit and at rest, with secure OEM-managed key-management controls subject to independent security assurance.'	Please refer addendum for the revised clause
2801		Cloud	6	Web Application Firewall shall be implemented on the cloud for Web based applications. WAF application signature should be updated and reviewed regularly. The Report shall be submitted to bank on a periodic interval.	Pre-Bid Query / Clarification: Since the proposed platform is an OEM-managed hosted security service, underlying WAF technology, signatures and configurations form part of the OEM's internal security architecture and may not be exposed as customer-specific reports. We request the Bank to accept periodic VAPT/penetration-test assurance or equivalent independent security assessment evidence covering the hosted application instead of WAF signature reports. Suggested Clarified Wording / Requested Action: The hosted web application/platform shall be protected through appropriate application-security controls. The OEM shall conduct periodic vulnerability assessment and penetration testing/security assessments and, subject to confidentiality restrictions, provide an executive summary/attestation or applicable independent assurance evidence to the Bank on request. Customer-specific WAF signature reports shall not be mandatory.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2802		Cloud	7	The systems in cloud infrastructure should be periodically updated with the latest anti-malware signatures, the bidder shall submit the periodic report on the same with bank.	Pre-Bid Query / Clarification: For an OEM-managed hosted security service, infrastructure anti-malware/endpoint controls are centrally managed and independently audited. We request the Bank to accept OEM security assurance and vulnerability/malware-control attestations rather than periodic host-level signature reports. Suggested Clarified Wording / Requested Action: The OEM shall maintain appropriate malware protection, vulnerability management, patching and security monitoring controls for the hosted infrastructure. Compliance may be evidenced through independent assurance reports/certifications and applicable security-control attestations instead of customer-specific anti-malware signature update reports.	Please refer addendum for revised clause
2803		Cloud	8	Data Loss Governance and risk management framework shall be defined by bidder for workload on the cloud and same shall be shared with bank on periodic basis. Data loss prevention controls should be implemented to secure the data in the cloud environment from unauthorized or inadvertent exfiltration.	Pre-Bid Query / Clarification: We request clarification that the requirement is intended to ensure protection against unauthorized/inadvertent data exfiltration through the proposed service and appropriate security controls for hosted customer data, rather than requiring disclosure of the OEM's internal cloud governance framework. Suggested Clarified Wording / Requested Action: The proposed solution shall provide configurable controls to identify and prevent unauthorized or inadvertent transmission/exfiltration of sensitive information through any channels. The OEM shall maintain appropriate access control, encryption and data-protection controls for customer data processed within the hosted service and provide applicable assurance documentation on request.	Please refer addendum for revised clause
2804		Cloud	9	Log generation, storage and review process should be certified by CERT IN empaneled auditor, report for the same shall be submitted by bidder as and when required by bank.	Pre-Bid Query / Clarification: For global SaaS/POD services, security logging and monitoring controls are typically independently audited under recognized assurance frameworks. We request the Bank to accept SOC 2 Type II/ISO 27001 or equivalent independent assurance in lieu of a mandatory CERT-In-empanelled audit of the OEM's internal log-generation/storage/review process. Suggested Clarified Wording / Requested Action: The OEM shall maintain documented security logging, monitoring, retention and review controls. Effectiveness shall be evidenced through applicable independent third-party assurance reports/certifications such as SOC 2 Type II, ISO 27001 or equivalent. CERT-In-empanelled audit may be required only for bidder-managed components deployed specifically within the Bank environment, where applicable.	Please refer addendum for the revised clause
2805		Cloud	10	IT Act 2000 & its amendments, and other Acts/Regulatory guidelines.	Pre-Bid Query / Clarification: Kindly clarify that the OEM must comply with legal/regulatory requirements applicable to it as the provider of the proposed hosted service and provide reasonable documentation to support the Bank's compliance obligations. Suggested Clarified Wording / Requested Action: OEM shall comply with applicable legal and regulatory obligations relevant to its provision of the proposed service and shall provide available security/privacy/compliance documentation reasonably required to support the Bank's applicable obligations.	Please refer addendum for the revised clause
2806		Cloud	11	CERT IN Empaneled auditor report's is required for the following:	Pre-Bid Query / Clarification: We request the Bank to permit internationally recognized independent assurance reports/certifications for OEM-managed hosted services. CERT-In empanelled audit reports may remain applicable to India-specific bidder-managed/on-premises components where such audit is feasible and required. Suggested Clarified Wording / Requested Action: For OEM-managed hosted/SaaS services, independent assurance reports/certifications such as SOC 2 Type II, ISO 27001 or equivalent shall be accepted. CERT-In empanelled audit reports shall be applicable only to components/services for which such India-specific audit is contractually and technically feasible.	Please refer addendum for the revised clause
2807		Cloud	12	The application and DB is/will be hosted separately on a dedicated infrastructure (physical/logical) for PSB. Evidence of dedicated infrastructure (physical/logical) for PSB should be submitted.	Pre-Bid Query / Clarification: The proposed platform is an OEM-managed hosted security service designed with logical access controls and customer data isolation. Requiring dedicated physical application/database infrastructure would restrict standard SaaS/POD architectures without necessarily improving the security outcome. We request acceptance of secure logical tenant/customer isolation supported by independent assurance evidence. Suggested Clarified Wording / Requested Action: The proposed hosted service shall provide secure logical segregation/isolation of Bank data and administrative access from other customers through appropriate access-control and tenant-isolation mechanisms. Dedicated physical application/database infrastructure shall not be mandatory where equivalent logical isolation is implemented and independently assured.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2808		Cloud	13	Feasibility to audit/review IT controls of the third party or obtaining independent review report for the same from CERT-In empaneled security consultant, to ensure it meets Bank's information security requirement.	Pre-Bid Query / Clarification: We request that the Bank permit review of current independent assurance reports/certifications as the primary mechanism for reviewing OEM IT controls. Any direct audit should remain subject to the OEM's standard contractual audit provisions, confidentiality, security, scope and advance-notice requirements. Suggested Clarified Wording / Requested Action: The Bank may review applicable independent third-party assurance reports/certifications covering the hosted service. Where additional audit is required, such audit shall be subject to mutually agreed scope, confidentiality/security restrictions, reasonable advance notice and the OEM's standard contractual audit provisions. A CERT-In empanelled consultant may review evidence made available under these conditions.	Please refer addendum for revised clause
2809	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 23	XSIAM	Point 18	The proposed solution shall provide cloud-native high availability and redundancy mechanisms to tolerate failures of underlying infrastructure components without disruption to security monitoring and operational capabilities. The solution shall provide automated failover and service continuity within the cloud environment through the CSP's native availability and resiliency capabilities	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. "" The proposed solution shall provide cloud-native redundancy mechanisms to tolerate failures of underlying infrastructure components without disruption to security monitoring and operational capabilities. The solution shall provide automated failover and service continuity "	Please refer the addendum for revised clause
2810	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 23	XSIAM	Point 36	The proposed solution must come with out-of the-box/customized to be delivered on day 1 support integration and dashboards, reports, rules etc. to provides rapid insights and operational visibility into large-scale CentOS, Windows, Unix and Linux environments machine data.: syslog, metrics and configuration files.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The proposed solution must come with out-of the-box/customized to be delivered on day 1 support integration and dashboards, reports, rules etc. to provides rapid insights and operational visibility into large-scale CentOS, Windows, Linux environments machine data.: syslog, metrics and configuration files.	No Change, Please be guided by the RFP
2811	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 24	XSIAM	Point 59	The proposed solution machine learning capabilities must allow addition or have inbuilt feature of custom machine learning algorithms from popular open-source libraries like NLP, Python etc.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The proposed solution must natively supports custom machine learning algorithms through its built-in Bring Your Own Machine Learning (BYOML) framework. This capability allows mature Security Operations Centers (SOCs) and security data scientists to access the massive security data lake stored within the platform and run bespoke analytics tailored to their specific environment.	No Change, Please be guided by the RFP
2812	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 37	XDR	Point 43	The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature or through seamless integration with a third-party sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature or through seamless integration with a third-party sandboxing solution from day 1.""	Please refer the addendum for revised clause
2813	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 1.4	Identity Threat Detection Solution must find and present high-risk attack pathways to critical IT assets	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. "ITDR provides identity risk context through User Risk View, Risk Management Dashboard, and identity alerts.	Please refer the addendum for revised clause
2814	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 1.6	Identity Threat Detection Solution should must automatically prioritize and remediate the riskiest identities to preemptively cut off what attackers need (and expect to find) to move undetected within the network.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. "ITDR identifies risky identities and supports remediation workflows for suspicious identity activity."	Please refer the addendum for revised clause
2815	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.3	The ITDR solution shall identify and assess exposed, improperly stored, or compromised credentials associated with user, privileged, service, and administrative identities on endpoints	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ITDR identifies risky identity posture, weak or compromised credentials, and suspicious activity involving user, privileged, service, and administrative accounts.	Please refer the addendum for revised clause
2816	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.4	Identity Threat Detection Solution should Identify, Misconfigured accounts, Legacy app accounts, Stale accounts, password policy violations, Kerberoastable credentials, unmanaged user accounts, unmanaged service accounts	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR identifies risky identity posture, weak or compromised credentials, Kerberoasting activity, and suspicious behavior involving service and administrative accounts""	Please refer the addendum for revised clause
2817	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.5	Identity Threat Detection Solution should Provide continuous monitoring and customizable, automated business rules to eliminate security policy violations, such as: • Stored credentials to sensitive assets • Local-admin accounts • Cached credentials stored in browsers, Windows and other systems	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR continuously monitors identity posture and access relationships to identify risky configurations, excessive privileges, and suspicious identity activity across Active Directory and related identity sources.""	Please refer the addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2818	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.7	Identity Threat Detection Solution should be available through rack-mountable on-premise deployment	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Identity Threat Detection Solution should be available through rack-mountable on-premise deployment not applicable for SaaS solution ""	Please refer the addendum for revised clause
2819	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.9	Identity Threat Detection Solution should detect all types of attack vectors including but not limited to pre attack reconnaissance,zero- day attacks, privilege escalation prevention, lateral movement, data theft	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR detects identity-based threats such as Active Directory reconnaissance, compromised accounts, privilege escalation, and anomalous access, while providing identity context to help investigate exposure and attack paths.""	The Clause is applicable only to idendity related threat vector only. The volumetrics is provided in the RFP and should be complied
2820	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.15	Identity Threat Detection controls should be able to automatically discover and flag hidden or shadow Tier 0 assets	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Identity Threat Detection and Response helps identify risky identity assets, excessive privileges, and exposure across identity relationships.""	Please refer the addendum for revised clause
2821	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 2.17	Identity Threat Detection Solution should be able to pull and analyze identity data from AD, Entra ID, identity stores, PAM systems	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR analyzes identity data from supported identity sources, including Active Directory and Microsoft Entra ID, to provide context on identities, permissions, and access exposure""	Please refer the addendum for revised clause
2822	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 3.4	The Identity Threat Detection Solution should integrate with compatible endpoint/extended detection solution to capture screen recordings or screenshots during active attacker sessions, as part of advanced forensic evidence collection	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR integrates with supported tools to share identity and endpoint context for investigation and response, including forensic collection where available.""	Please refer the addendum for revised clause
2823	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 52	ITDR	Point 3.5	The Identity Threat Detection Solution should integrate with compatible network detection solution to support collection of PCAP data to support network-level visibility of the incident	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR integrates with supported tools to share identity risk context and support investigation workflows, including network-related telemetry where available.""	Please refer the addendum for revised clause
2824	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 53	ITDR	Point 3.7	Identity Threat Detection Solution should, as part of its forensic data collection process, include detailed attack path information, including the protocols leveraged during the attack.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR provides identity context through asset, permission, and authentication analysis, and detects identity-based threats such as compromised accounts, privilege escalation, anomalous access, and Active Directory reconnaissance.""	Please refer the addendum for revised clause
2825	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 53	ITDR	Point 3.9	Identity Threat Detection solution should detect an adversary's attempt to move laterally toward the organization's key assets using as many hosts (Windows, Mac, or Linux) as possible in the organization without requiring a persistent agent.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Identity Threat Detection solution should detect an adversary's attempt to move laterally toward the organization's key assets using as many hosts (Windows, Mac, or Linux) as possible in the organization With or without requiring a persistent agent.""	Please refer the addendum for revised clause
2826	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 53	ITDR	Point 3.10	Identity Threat Detection Solution should collect user and computer information from Active Directory as part of its forensic data gathering to enhance context and assess risk exposure. detect at the earliest point in the attack, post initial compromise as the attacker is first attempting to move laterally and escalate privilege.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""ITDR collects and analyzes identity data to improve context and assess risk exposure. It detects identity-based threats, including compromised accounts, privilege escalation, anomalous access, and Active Directory reconnaissance, early in the attack path.""	Please refer the addendum for revised clause
2827	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 53	ITDR	Point 3.11	Identity Threat Detection Solution should collect user and computer data from Active Directory during forensic data gathering to improve context and evaluate risk exposure, while ensuring that all deception techniques remain hidden from legitimate users.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Identity Threat Detection and Response collects and analyzes identity data to improve context and assess risk exposure. It provides deep visibility into identity assets, permissions, relationships, and authentication activity across Active Directory and other identity sources. ITDR also supports forensic investigations through endpoint data collection and analysis."	Please refer the addendum for revised clause
2828	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 19	CTEM	Point 7	Each intelligence item should include metadata such as date, author, source, and pre-classification of raw data	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Intelligence items include enriched context, source information, and analysis metadata to support investigation and prioritization.""	Please refer the addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2829	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 19	CTEM	Point 11	The solution/service should generate investigation reports for designated VIPs or other high-risk identities/assets, providing an overview of identified digital exposure and associated risk.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution provides risk context and investigation views for identities and assets, helping analysts assess exposure and related risks.""	No Change, Please be guided by the RFP
2830	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 19	CTEM	Point 19	The solution should detect compromised credentials for employees and VIPs, exposed payment card information, and aggregate data from known breach databases in real time	Kindly Remove this clause for larger participation	Please refer addendum for revised clause
2831	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 20	CTEM	Point 38	The solution should be deployed agentlessly, without requiring sensors or agents on endpoints, servers, or network appliances	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution should be deployed agentlessly, With or without requiring sensors or agents on endpoints, servers, or network appliances""	S.No 38 Please refer addendum for revised clause The solution should be deployed agent/agentlessly, without requiring sensors or agents on endpoints, servers or network appliances.
2832	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 81	ASM	Point 6	The visual representations should be downloadable in PDF, JPG, PNG and other generally used formats	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution supports exporting reports and data views in supported file formats such as PDF, CSV, TSV, JSON, or ZIP, depending on the workflow""	No Change, Please be guided by the RFP
2833	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 81	ASM	Point 8	The solution shall provide information on vulnerabilities, misconfigurations, insecure configurations, obsolete or unsupported technologies, applications, services, URLs, ports, network components, systems, databases and other relevant infrastructure that are publicly exposed or otherwise identifiable through authorized discovery and assessment activities.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution provides exposure information for internet-facing assets, including vulnerabilities, misconfigurations, services, and related attribution data discovered through authorized asset mapping and assessment.""	Please refer addendum for revised clause
2834	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 81	ASM	Point 9	The solution should provide data/information on security flaws/ inherent vulnerabilities (allegedly) reported about the digital products exposed to the Internet (For example: internet banking, mobile applications) offered to the bank's customers, as leaked in public domain, or other forums	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution provides exposure and risk information for internet-facing digital assets, including vulnerabilities, services.""	No Change, Please be guided by the RFP The requirement is intended to provide visibility not only into directly identified technical vulnerabilities but also into relevant security information concerning the Bank's internet-facing digital products
2835	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 81	ASM	Point 10	The solution shall identify and provide relevant information on potentially exposed sensitive information associated with the Bank, including source-code references, code snippets, API information, credentials, keys and other security-relevant information, where such information is identifiable through publicly available sources, external attack-surface intelligence or other authorized discovery mechanisms.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution provides exposure information for internet-facing assets, including vulnerabilities, misconfigurations, code weaknesses, and exposed secrets discovered through attack surface.""	Please refer addendum for revised clause
2836	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 54	Cloud security	Point 4	The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud environment like AWS/Azure/GCP/Meghdoot, AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud environment like AWS/Azure/GCP/, AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.	The requirement is intended for identification and contextualization of potentially exposed sensitive information associated with the Bank
2837	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 55	Cloud security	Point 9 (Sub point)	○Automatic, in-product remediation via the Cloud Service Provider (CSP) API (1-click)	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""The solution supports in-product remediation workflows, including automated actions and approval-based playbooks where configured.	Please refer the addendum for revised clause
2838	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 56	Cloud security	Point 25	The solution must provide an self-service portal for engineers. The admin portal should be able to define the eligibility for users and groups, based on role, scope and duration. The solution should provide approval workflow and audit logs	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation." The solution supports granular access control, human approval in select workflows, and audit logging for access-related changes.	Please refer the addendum for revised clause
2839	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 40	NDR	Point 9	Easy-to-manage, clientless platform that deploys quickly and involves minimal or no dependency on customization and management.	We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. ""Easy-to-manage, clientbase clientless platform that deploys quickly and involves minimal or no dependency on customization and management.""	Please refer the addendum for revised clause
2840	RFP Pg 35	Deployment Pattern	Point d	NDR: The NDR solution shall be deployed On-Premises within the Bank's DC and DR, with the required brokers, aggregators, collectors and/or enforcement components configured in N+N Active-Active configuration at both sites.	The proposed NDR solution shall utilize a hybrid deployment model or SaaS model.With the required brokers/ aggregators/collectors /Sensors and enforcement components configured in N+N Active-Active or Active- Passive configuration at both sites DC and DR.	Please refer addendum for the revised clause
2841	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 40	NDR			Clarification: Kindly confirm the specific physical interface type and speed the Bank will provide for the uplink to the NDR sensor.	Details shall be shared with successful bidder

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2842	APPENDIX 1A Functional Compliance Sheet (Solutions), Page 40	NDR	Point 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	"We kindly request an amendment to Clause as proposed below. This modification will facilitate wider bidder participation. "" The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead.""	Please refer Addendum for revised clause
2843	SELECTION OF BIDDER FOR SUPPLY INSTALLATION, IMPLEMENTATION, MAINTENANCE & MANAGEMENT OF NEXTGEN SOC & RELATED SERVICES BID NO: PSB/HO-CISO CELL/2026-27/RFP_01 DATED 09/09/2026 Page 68	7.7 On-cloud proposed solution OEM Responsibilities	Page 8	The solution shall support secure connectivity with the Bank's on-premises infrastructure,cloud environments, and external systems through private and secure communication mechanisms.	SIEM is a SaaS solution accessible over the internet using passwords and multi-factor authentication and Https. However, access to your Cortex XSIAM tenant can be restricted based on your Bank's static public IP addresses. Kinkdy change this clause to "" The solution shall support secure connectivity with the Bank's on-premises infrastructure,cloud environments, and external systems through private or secure communication mechanisms via internet or tenant can be restricted based on Bank's static public IP addresses..""	Please refer the addendum for revised clause
2844	RFP Pg 33	Section 7.2.3 Deployment Model Definition		CSP-hosted components shall provide cloud-native High Availability (HA), geographic resiliency and DR in accordance with the SLA, RTO and RPO requirements specified in this RFP.	Cortex XSIAM is pure SaaS Solution hence this clause is not applicable. kindly remove this for SaaS offerings.	Please refer addendum for the revised deployment architecture
2845	RFP Pg 41	7.3.1.1 Modules, Architecture & Deployment:	Point 7	All SIEM components, including collectors, ingestion nodes, correlation engines, processing nodes, etc., are deployed in the prescribed HA architecture irrespective of whether they are deployed at the Bank's Data Centre (DC), Disaster Recovery (DR) Centre, CSP Primary Site, or CSP Secondary Site.	Not applicable, as Cortex XSIAM is a SaaS solution. However, the on-premises Cortex Broker VM component can be deployed in a High Availability (HA) configuration across primary Data Center (DC) and Disaster Recovery (DR) sites	For SaaS-based components, the applicable SaaS SLA shall specify the required uptime/availability commitment. For components deployed at the Bank's DC/DR, the prescribed HA architecture shall apply as specified in the RFP
2846	RFP Pg 43	7.3.2.2 Key Deliverables	Point 7	Backup, retention, restoration, documentation and knowledge transfer for configured security automation capabilities and use cases.	Need more clarification on this clause	No Change, Please be guided by the RFP Refer Section7.2.4.3 Storage and other Requirement
2847	35	7.2.4.1 Deployment Pattern		SIEM, SOAR and UEBA: The core platforms shall be deployed in the Cloud/SaaS environment, with the required brokers, collectors, aggregators and/or integration/enforcement components deployed at the Bank's DC and DR in N+N Active- Active configuration.	Industry standard DC - HA - DR are active-passive or primary-standby to optimise the hardware allocation as well as optimal use of overall resources allocated. Please make changes to allow active-passive architecture supported.	No Change, Please be guided by the RFP
2848		Section 10: EVALUATION CRITERIA		The proposed OEM SIEM Solution with a minimum capacity of 30,000 EPS or 1.2 TB/day shall have been successfully implemented and be under management/maintenance in at least one (1) BFSI in India. and The proposed OEM SIEM Solution with a minimum capacity of 30,000 EPS or 1.2 TB/day shall have been successfully implemented on cloud in one (1) in India	For wider particiaption of SIEM vendors and us to qualify, can you please allow customer with 30,000EPS on-premises to meet the stated condition as per the RFP.	Please refer addendum for revised clause.
2849	1	Primary Storage	5	Proposed storage solution should be offerred with minimum 2 controllers with minimum 256 GB DRAM Cache memory on the entire storage Solution. The solution should scale to atleast 512GB Cache memory by adding additional controller.	Change To: Proposed storage solution should be offerred with minimum 2 controllers with minimum 128 GB DRAM Cache memory on the entire storage Solution. The solution should scale to atleast 256GB Cache memory by adding additional controller. Explaination: Cache ask should be Reduced as cache of 64GB or less per controller (128GB total) is enough as the latest CPUs, high-speed memory, and Gen 5 PCIe cards deliver the required performance efficiently. Modern storage controllers optimize cache usage, and industry benchmarks confirm that asked performance can be achieved with lower memory. This reduction not only meets technical needs but also decreases hardware, power, and cooling costs, resulting in a lower TCO for the solution	No Change, Please be guided by the RFP
2850	1	Backup Solution	16	The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data over a secure, API-based disk-to- disk (D2D) connection.	Change To: The proposed disk-based storage/appliance must interoperate with industry-leading server platforms and operating systems, and must ingest backup data using standard Data protocolos such as FC, ISCI, NFS, S3 Expalination: This specific ask qulifies only specific backup appliance not any target storage as enterprise storage do not support data ingestion using API rather laverage protocols such as FC, ISCI, NFS, S3.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2851	1	Backup Solution	25	The Proposed Appliance/Backup Storage must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism	Change To:The Proposed Appliance/Backup Solution must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism Explaination: Proposed ask should be from Solution instead of storage as any storage does not offer file-level checksum reporting for backup files. This is typically a function of the backup software (e.g., Commvault, Veeam) that stores backups on storage.	Please refer addendum for revised clause
2852	1	Primary Storage	21	If the OEM proposes effective storage capacity, then DRR should be applicable for the entire contract period. Incase, the DRR is not achieved anytime during the contract period, the OEM is liable to supply the additional drives/capacity to meet the required performance and effective capacity at no additional cost to the bank.	Query:Bank should provide workload details such as if data would encrypted or non-encrypeted, compressed or non-compressed and type of DB, VM etc. Explaniation: It would help OEM to size solution with correct DRR commitment.	Bidder/OEM shall assess the workload details and other relevant technical requirements and propose a suitably sized and architected solution meeting all requirements & terms of the RFP. The Bidder/OEM shall be responsible for sizing, performance, interoperability and adequacy of the proposed solution
2853	1	Long Term Storage		Addititional Point Request	Point to be written as: Long Term Storage should support WORM (Wrte Once, Read Many) capability to have Data Immutability. Explaination: We recommend implementing WORM (Write Once, Read Many) capability for long-term backup storage to ensure data is protected against accidental deletion and ransomware attacks. Additionally, WORM functionality is required to comply with regulatory guidelines for banking institutions. Since backup storage is expected to provide WORM capability, long-term backup storage should also comply with this requirement to maintain robust data protection.	As per tender pg no. 39, point a, "No Bank data shall be deleted or made inaccessible before expiry of the applicable retention period (refer annexure 21) and without explicit written authorization from the Bank" It is bidders responsibility to ensure that they comply with the tender requirement
2854	1	Primary Storage Backup Storage Long Term Storage		New Point request	Point to be written as: The proposed storage systems (for all 3 storage requirements), should have launch dates within past 3 years Explainations: We recommend qualifying storage systems with a launch date within the past three years. This approach ensures a better return on investment and reliable long-term support for a period of 7 to 10 years, as required by the bank. Some OEMs are currently offering systems that are over six years old and lack a clear roadmap or support commitment, which poses a risk to long-term operational stability and longitivity.	Please refer addendum for revised clause.
2855	7	1 KEY INFORMATION	Security Deposit/Earnest Money deposit	Rs. 4.25 Crore (INR Four Crore and Twenty-Five Lakh Only)	Considering the objective of encouraging wider participation from established and technically capable System Integrators, we request the Bank to kindly rationalize the EMD from INR 4.25 Crore to INR 1 Crore. The proposed reduction would facilitate participation by capable bidders while continuing to provide adequate financial safeguards to the Bank through the prescribed Performance Guarantee and other contractual remedies.	No Change, Please be guided by the RFP
2856	140	13.1 Service Level Agreement	13.1 Service Level Agreement – Clause 6	For SLA and penalty calculations, downtime shall be measured from the time the Bank/bank's appointed vendor reports the incident to the bidder until the time the bidder notifies the Bank that the issue has been resolved, and normal services have been restored, subject to verification by the Bank.	Kindly clarify the detailed downtime/SLA measurement methodology, including treatment of planned maintenance windows, Bank/CSP/network dependency outages, force majeure, third-party service outages, and incidents not attributable to the bidder.	No Change, Please be guided by the RFP
2857	158	13.3 At-Risk Amount	13.3 At-Risk Amount	The monthly At-Risk Amount (ARA') shall be 15% of the estimated monthly payout of the respective month.	Kindly clarify whether the At-Risk Amount (ARA) of 15% of the estimated monthly payout is intended as a temporary withholding mechanism and whether any amount withheld under ARA will be adjusted against applicable LD/SLA penalties. Kindly also confirm that there will be no duplicate recovery for the same underlying event.	The At-Risk Amount is a contractual performance mechanism and shall be withheld/adjusted in accordance with the applicable performance requirements specified in the RFP. It shall not automatically be treated as an additional penalty or Liquidated Damages (LD). Any withholding, adjustment or recovery under the At-Risk Amount shall be accounted for within the overall 10% penalty/LD cap specified in Section 13.2 and shall not be over and above such cap.
2858	136	12 PAYMENT TERMS	12 PAYMENT TERMS	The selected Bidder will have to submit the documents (Delivery challans with all the part codes of OEM which shall be reconciled with BOM) at the Bank's office along with a request letter for payment. No advance payment will be made. Payment will be made in Indian Rupees only. All taxes to be paid will be subject to GST applicability. TDS will be applicable.	Considering the substantial upfront procurement and OEM/cloud subscription commitments, kindly consider allowing payment against successful delivery and verification of hardware/software licenses, with the balance linked to UAT/Go-Live milestones.	No Change, Please be guided by the RFP
2859	159	13.5 Subcontracting	13.5 Subcontracting	The bidder shall not subcontract or assign the whole or any part of the Contract to any third party without the prior written consent of the Bank.	Kindly clarify whether specialized offsite managed security services (such as dark web monitoring, brand protection, phishing simulation, threat intelligence feeds or continuous red teaming) may be delivered through an OEM/service provider engaged and contractually backed by the bidder, provided the bidder remains fully responsible and accountable to the Bank.	No Change, Please be guided by the RFP
2860	98–99	9 PROJECT TIMELINES	Overall Implementation period shall be 5 Months (Start Date is T0)	Overall Implementation period shall be 5 Months (Start Date is T0) for all solution & services	Given the dependencies on Bank-side infrastructure, access, network readiness and third-party/OEM prerequisites, kindly confirm that the five-month implementation timeline will be measured from timely availability of the required Bank prerequisites and approved access/dependencies, and that delays attributable to dependencies outside the bidder's control will not be considered for levy of LD.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2861	20 / 21	6.10 EMD / 6.11 Performance Guarantee	6.10 Earnest Money Deposit (EMD) / 6.11 Performance Guarantee	EMD shall be furnished by way of Bank Guarantee drawn on a Scheduled Bank in India, except cooperative bank, RRB and PSB, in favour of PSB payable at Delhi. / Performance Guarantee shall be submitted by way of Bank Guarantee in favour of PSB payable at Delhi.	As per applicable GeM/Government procurement guidelines, Insurance Surety Bond is an accepted form of Bid Security/EMD and Performance Security. Kindly confirm that the Bank will permit an Insurance Surety Bond (Surety Bond) from an eligible/authorized insurer, in addition to Bank Guarantee, for furnishing both the EMD and Performance Security/PBG under this RFP. Kindly also confirm that the prescribed validity, claim period, invocation terms and other conditions applicable to the Bank Guarantee will be equally applicable to the Insurance Surety Bond.	6.10 - Please refer addendum for revised Clause 6.11 - No Change, Please be guided by the RFP
2862	182	16.5 Annexure 5 Pre Qualification Criteria	16.5 Annexure 5 Pre Qualification Criteria	Bidder must have at least enrolled manpower (on bidder's payroll) of 100 experienced employees skilled in areas of Cyber security.	Kindly modified the clause as "Bidder must have at least enrolled manpower (on bidder's payroll) of 50 experienced employees skilled in areas of Cyber security."	No Change, Please be guided by the RFP
2863	35 of 122	XDR	4.13	The goal is to minimize the attack surface by continuously monitoring, updating, and provide compensatory controls for vulnerabilities and exploits in the endpoints	We request to modify this clause as below "The goal is to minimize the attack surface by continuously monitoring, updating, and provide visibility for vulnerabilities and exploits in the endpoints" Justification: The term "visibility" is outcome-focused and technology-agnostic, allowing solutions to detect and report vulnerabilities through various mechanisms (signatures, behavioral analysis, real-time scanning, etc.), whereas "compensatory controls" is overly prescriptive and implies specific mitigation techniques that may not be applicable to all vulnerability types or endpoint environments. Changing to "visibility" maintains the security intent while enabling bidders to propose diverse, fit-for-purpose solutions without unnecessary implementation constraints.	No Change, Please be guided by the RFP
2864	35 of 122		12	The proposed solution must provide protection against malicious AI application tampering on the endpoints	We request to modify this clause as below "The proposed solution must provide protection against malicious applications tampering on the endpoints" Justification:The "AI" qualifier is overly specific and may exclude non-AI malware threats, creating coverage gaps. The broader term "malicious application tampering" aligns with industry-standard endpoint protection language and ensures comprehensive threat protection regardless of the attack vector or technology employed.	No Change, Please be guided by the RFP
2865	36 of 122		15	The proposed XDR solution must provide comprehensive activity data management and search capabilities, including receiving activity data in the form of telemetry, and metadata; feature for automatic query runs and email notifications; threat matching features using Boolean Logic and other criteria; and options to export, import, delete, and share saved search queries.	We request to modify this clause as below: The proposed XDR solution must provide comprehensive activity data management and search capabilities, including receiving activity data in the form of telemetry, and metadata; feature for automatic query runs and email notifications; threat matching features using Boolean Logic and other criteria; and options to export, delete, and share saved search queries. Justification:The "import" functionality is not a core operational requirement for XDR activity data management. The primary requirements are exporting queries for backup/sharing, deleting obsolete queries, and sharing queries among team members—all of which are standard XDR capabilities. Import functionality introduces unnecessary complexity, potential security/governance risks from external query sources, and is not universally supported across commercial XDR solutions, thereby limiting vendor options unnecessarily	No Change, Please be guided by the RFP
2866	36 of 122		22	The solution should offer options to leverage anti-malware and anti-spyware components stored locally on agents, or signatures stored in-the-vendor cloud	From the operational context and use cases for each deployment option, ensuring continuity of threat protection in all connectivity scenarios. By explicitly defining "when offline" (local components) and "when online" (cloud signatures), the clause removes ambiguity regarding the solution's capability to maintain protective coverage during network disconnections while leveraging updated threat intelligence when connectivity is available We request to modify this clause as below "The solution should offer options to leverage anti-malware and anti-spyware components stored locally on agents when offline, or signatures stored in-the-vendor cloud when online."	No Change, Please be guided by the RFP
2867	36 of 122		29	The solution Device Control capability must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The solution Device Control capability must support Network Devices, USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, time based device control capabilities allowing admin to define the policy specifically for the endpoint operating systems (Windows 10, 11 or higher).	We request to modify the clause as below: The solution Device Control capability must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The solution Device Control capability must support USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, allowing admin to define the policy specifically for the endpoint operating systems (Windows 10, 11 or higher)to allow the devices as required. Justification: Network Devices are typically managed through enterprise network security controls and firewalls rather than endpoint Device Control, and time-based controls create unnecessary operational complexity and maintenance overhead. The modified clause focuses on high-risk local device vectors (USB, Mobile Storage, Bluetooth, Modems) that pose direct security threats to endpoints, while allowing flexibility for organizations to enable specific devices based on business requirements.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2868	37 of 122		43	The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature or through seamless integration with a third-party sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data	We request to amend this clause as below: The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data. Justification: To ensure operational independence and reduce implementation complexity, the organization requires native sandbox functionality built into the core solution rather than relying on third-party integrations, which introduce external dependencies, potential single points of failure, and increase support overhead. This modification mandates that bidders deliver complete sandboxing capability as an integrated component from day 1, ensuring seamless functionality, consistent vendor accountability, and simplified maintenance and support operations without external vendor coordination.	Please refer addendum for revised Clause
2869	38 of 122		57	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	We request to amend this clause as below: The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture or 99.9% availability SLA distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead. Justification: The modification provides architectural flexibility while maintaining the Bank's core availability objective. Not all qualified SaaS vendors employ Active-Active multi-AZ architecture; however, industry-standard 99.9% SLA meets enterprise-grade requirements and enables broader vendor participation without compromising operational resilience. This alternative approach is vendor-agnostic, measurable, and backed by contractual guarantees rather than architectural prescriptions.	Please refer Addendum for revised clause
2870	37 of 122		42	The proposed solution should provide recommended actions to address and mitigate threats detected on endpoints. These remediation suggestions should be informed by forensic data collected from endpoints and detailed analysis performed by the solution to enhance threat response and resolution.	To ensure accurate cost proposals and licensing calculations, please clarify the estimated forensics data volume requirements: a) What is the expected monthly forensics data volume (in GB) that the solution must support? b) What is the planned retention period for forensics data? c) Does this volume include forensics data from all sources (endpoints, servers, cloud workloads, network) or specific sources only? This clarification will enable all bidders to calculate appropriate licensing models and provide consistent cost estimates	Details shall be shared with the successful bidder
2871	54 of 122	Cloud Security	4	The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud envirionment like AWS/Azure/GCP/Meghdoot, AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.	We request to modify this clause as below The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud envirionment like AWS/Azure/GCP/ AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports. Justification: Meghdoot is a comprehensive open-source cloud suite, but bringing it up to PSB requirements demands significant development and integration effort. To be effective, the target cloud environment must be seamless, eliminating the overhead of custom modifications.	Please refer addenudm for revised clause The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud envirionment like AWS/Azure/GCP, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.
2872	Addition of Point as recommendation	Cloud Security	To be Added in Cloud Security	The proposed solution should also support the File scanning with no limitation on file/object type or size covering application across organisation. This should include but is not limited to Amazon Simple Storage Service (S3), Amazon FSx amd Amanzon Elastic File System.	Benefit to PSB: Comprehensive file scanning eliminates critical security blind spots across the organization's cloud storage infrastructure, ensuring no malware, ransomware, or sensitive data can be inadvertently stored in S3, FSx, or EFS without detection. By removing file type and size limitations, the solution prevents attackers from bypassing scanning through obfuscation or leveraging uncommon formats, while the multi-storage coverage consolidates security posture across diverse AWS storage services under a single unified policy. This provides unified threat visibility, enables regulatory compliance (HIPAA, PCI-DSS, GDPR), prevents data exfiltration, and protects against insider threats and supply chain compromises affecting cloud-stored data—significantly reducing the risk of ransomware attacks, compliance violations, and unauthorized data exposure.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2873	page 30 of 273	Extended Detection & Response (XDR)	5	Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Cloud (SaaS): HA Deployment aligned with the SLA, RTO & RPO (Refer Section 13). Management Console: Deployed at both Primary and Secondary sites	We request to amend this clause as below: Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Cloud (SaaS): HA Deployment aligned with the SLA, RTO & RPO (Refer Section 13). Justification: In Appendix 1A clause 27 under XDR explicitly mention for SaaS "ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead" Though it's a SaaS based the management console cannot be deployed at both primary and secondary sites.	Please refer addendum for revised clause
2874	page 31 of 273	Cloud Workload Protection Platform (CWPP)	13	Cloud (SaaS): Deployment aligned with the SLA, RTO & RPO (Refer Section 13).. Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Management Console: Deployed at both Primary and Secondary sites	We request to amend this clause as below: Cloud (SaaS): Deployment aligned with the SLA, RTO & RPO (Refer Section 13).. Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Justification: For SaaS solution the management console cannot be deployed at banks primary & secondary site	Please refer addendum for revised clause
2875	Page 38 of 122 & Page 38 of 122	XDR	22 to 35	These points are duplicate need to be removed	These points are duplicate need to be removed	No Change, Please be guided by the RFP
2876	29, 35 & 259	Sections 7.2.1, 7.2.4.1(b) & 16.21.2	Section 7.2.1 (Deception Technology): "Any agent/Enforcer/Deceptor Standalone at DC and HA, N+N, Standalone at DR." Section 7.2.4.1(b): "The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active	Deception deployment and high-availability topology	The RFP describes the Bank-side deception components as standalone in Section 7.2.1, point no.- 4, but it is also mentioned HA and N+N. We request the bank to kindly clarify that in case we're deploying the solution on-prem, whether Bank needs the solution in Standalone mode/HA mode/N+N mode. Section 16.21.2 (Decoy), point no.-8, Bank has asked that all the inline components of solution should be in HA mode with automatic failover capability. However, the deception solution is not inline. Hence, we request Bank to clarify if they need the Deception Solution in HA. We request the Bank to add on-prem solution also in addition to Cloud/SAAS+Hybrid.	Please refer addendum for revised clause
2877	45, 261 & 262	Sections 7.3.6.2(2) & 16.21.3 - Deployment and Data Retention	Section 7.3.6.2(2): "Restore the logs/data from backup for forensic investigation and as per bank requirement without any additional cost." Section 16.21.3: "Duration of the Contract (Monthly Full backup) - Long-Term Storage (LTS) - Entire Duration of the Contract." The RFP further states that applicable Monthly Full Backups shall be	Backup, restoration and log-retention requirements	We request bank to kindly confirm that if the bank will provide the storage for backup.	No Change, Please be guided by the RFP. Bidder to right size and provide all the required infrastrcuture as per RFP
2878	68	Section 7.7 - On-cloud proposed solution OEM Responsibilities, Point 10	"The OEM shall have valid ISO/IEC 27001 certification and SOC 2 Type II report."	Cloud OEM certification requirement	We request the bank to accept ISO/IEC 27001 or SOC 2 Type II or both.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2879	29, 32 & 35	Sections 7.2.1, 7.2.3 and 7.2.4.1(b)	Section 7.2.1 (Deception Technology): "Cloud (SaaS) + Hybrid" Section 7.2.3: "The solution shall be hosted through a Cloud Service Provider (CSP), either fully as a SaaS service or through a combination of CSP-hosted and Bank-hosted components." Section 7.2.4.1(b): "Deception Technology: The core Deception platform shall be deployed in the	Responsibility for providing the Cloud/SaaS environment	7.2.4.1(b) We request the bank to kindly add the on-prem implementation option also for the core component of the Deception Solution.	Please refer addendum for revised clause
2880	35 & 91	Sections 7.2.4.1(b) and 7.18.1 - Compute Infrastructure, Point 1	Section 7.2.4.1(b): "Deception Technology: The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active configuration. The Cloud/SaaS deployment shall be aligned with the applicable SLA, RTO and RPO requirements."	Hardware and VM infrastructure for Bank-hosted deception components	We request the bank to kindly add the on-prem implementation option also for the core component of the Deception Solution.	Please refer addendum for revised clause
2881	84	Breach and Attack Simulation (BAS)	Sl. No. 1 - Technical Specification	The solution should simulate Ransomware Attacks	Rationale for change: The clause as drafted is a single unqualified statement that every bidder in this category will mark compliant, so it cannot differentiate responses against the 10 marks allotted. It also does not define what constitutes a ransomware simulation. A ransomware validation exercise is only meaningful to the Bank if the platform reproduces the tradecraft ransomware operators actually use, including vulnerable driver loading to terminate endpoint protection, and does so without causing damage on production assets. The Bank is requested to replace the clause with testable criteria covering safe execution of destructive behaviours, deterministic cleanup, and kernel-level attack testing. Proposed modified clause: The proposed solution must execute structurally authentic attacks with destructive elements neutralised, and must be able to trigger destructive-technique detections without the harmful action (for example, testing volume shadow copy deletion detection without deleting the volume shadow copy). It must provide deterministic cleanup mechanisms, safe for execution on production assets, including backup, restore, and removal of all artifacts across: a. File b. Registry c. Service	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2882	84	Breach and Attack Simulation (BAS)	Sl. No. 3 - Technical Specification	The ability to simulate infiltration techniques for breaching a network or infecting a host	Rationale for change: "Infiltration techniques" is undefined and cannot be evaluated objectively. Initial access is the stage at which the Bank's email gateway, secure web gateway and web application firewall are tested, and current adversary tradecraft delivers initial access through container formats such as ISO, IMG, MSI, LNK and ZIP, followed by execution that avoids system interpreters in order to bypass AMSI, script block logging and constrained language mode. A clause that names these delivery and execution requirements allows the Bank to compare bidders on demonstrable capability rather than on a general claim. Proposed modified clause: The proposed solution must dynamically generate container-format payloads including ISO, IMG, MSI, LNK, and ZIP variants containing executables, shortcuts, or DLL hijack chains, and deliver them via uniquely generated URLs per simulation to comprehensively validate email gateway, secure web gateway, and WAF filtering against modern initial-access techniques such as ISO-LNK-DLL chains. The simulation agent must execute malicious behaviours and adversary techniques without reliance on system interpreters including PowerShell, CMD, BASH, or SH, validating control effectiveness against modern adversary tradecraft that increasingly avoids interpreter-based execution to bypass AMSI,	No Change, Please be guided by the RFP
2883	84	Breach and Attack Simulation (BAS)	Sl. No. 6 - Technical Specification	The solutions should test Security Operations Center (SOC) detection capability of bank by simulating multi-chained payloads with advanced evasion methods including DLL Hijacking, Process Injection, and PPID spoofing for breaching and infiltrating the network.	Rationale for change: The clause names only three evasion techniques and does not state that they must be executed as real behaviours on the asset rather than logged as simulated steps. SOC detection validation succeeds or fails on two things the clause does not capture: whether the payload natively performs modern evasion against the deployed control stack, and whether each technique is available in multiple procedure variants, since a detection that catches one implementation of LSASS credential dumping routinely misses six others. The Bank is requested to expand the clause so that detection coverage is validated across the attacker variant space. Proposed modified clause: The simulation payload execution must natively perform the following techniques as executed behaviours against the deployed control stack: a. EDR unhooking (NTDLL unhooking, direct and indirect syscalls) b. Reflective DLL injection c. Process hollowing d. PPID spoofing e. Command-line argument spoofing f. Fileless in-memory execution For each in-scope MITRE ATT&CK technique, the proposed	No Change, Please be guided by the RFP
2884	84	Breach and Attack Simulation (BAS)	Sl. No. 7 - Technical Specification	The solution should have the ability to create custom use cases / simulations attacks according to bank's requirement.	Rationale for change: As drafted the clause is satisfied by a script upload field or by a vendor professional services engagement, both of which leave the Bank dependent on the OEM for every new scenario and carry recurring cost. For the Bank's own security team to build scenarios for proprietary applications and internal workflows, the clause should require a user interface driven attack creator with named configurable parameters. Proposed modified clause: The proposed solution must provide a UI-driven attack creator enabling customer security teams to design custom multi-stage simulations with configurable name, description, MITRE category, execution privileges (User/Admin), payload type (DLL/EXE/Service/ISO/MSI/LNK), and chained secondary behaviours supporting organisation-specific scenario testing for proprietary applications, internal workflows, and bespoke attack hypotheses.	No Change, Please be guided by the RFP
2885	84	Breach and Attack Simulation (BAS)	Sl. No. 8 - Technical Specification	The solution must allow the execution of simulations on multiple agents simulataneously. An attack chain must be executed on multiple endpoints agents at the same time to provide unique attack specific insights across the deployed agents in the organisation.	Rationale for change: The clause states the requirement for simultaneous execution but does not exclude sequential execution presented as a single campaign, which is how several solutions in this category operate. It also does not address the operational prerequisites for running simulations across a bank-scale estate: the agent must be deployable at scale through Group Policy or golden image, must run silently so that branch and business users are not alerted or disrupted, and must update centrally without re-imaging or desk visits. The Bank is requested to make both the concurrency model and the deployment model explicit. Proposed modified clause: The proposed solution must execute a single coordinated attack campaign across multiple agents, business units, and geographies simultaneously, not sequentially (i.e. One Kill chain, run on multiple Endpoint Targets at the same time), producing independent per-agent evidence consolidated into a unified campaign report. Solutions that walk through agents one-by-one cannot realistically validate enterprise-scale concurrent compromise scenarios. The simulation agent must be a lightweight software package suitable for enterprise mass-deployment via Group Policy Object (GPO), golden image baking, or standard endpoint management tooling, requiring no per-host configuration post-installation.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2886	84	Breach and Attack Simulation (BAS)	Sl. No. 11 - Technical Specification	The solution should support technical integrations with bank's existing solutions (e.g., SIEMs, ticketing systems, log management, Firewalls, automation/orchestration, analytics solutions, threat intelligence solutions, etc.)	Rationale for change: "Should support technical integrations" is unverifiable and is routinely answered with roadmap commitments or bespoke development quoted after award. For closed-loop validation, where a simulation result is correlated against the alert raised in the Bank's SIEM and a ticket is created automatically, the Bank needs a documented API, automation tooling and pre-built connectors available at the time of bid. The Bank is requested to make the integration requirement specific and verifiable. Proposed modified clause: The proposed solution must expose a RESTful API with publicly available OpenAPI documentation, provide an open-source CLI and SDK for automation, and ship pre-built integrations with major SIEM, SOAR, ITSM, EDR, firewall, and email gateway vendors to enable closed-loop validation of alerts, automated ticket creation, and detection correlation.	No Change, Please be guided by the RFP
2887	30	RFP - 7.2 Solution & Services Deployment Model and Their HA Requirement 7.2.1 Solutions – Master Deployment Matrix	6. Network Detection & Response (NDR)	Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Management Console: Deployed at both DC and DR	Different NDR solution works on different redundancy deployment methodology (I.e Active - Active or Active - Passive). Request bank to modify the clause as: Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active/Passive at DC and HA, N+N, Active-Active/Passive at DR. Management Console: Deployed at both DC and DR	Please refer addendum for revised clause
2888	45	RFP - Scope of Work 7.3.5 Network detection and response (NDR)	7.3.5.1 Modules, Architecture & Deployment:	Pt 2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Generally NDR solutions are deployed with sole purpose of doing network analysis, threat detection & response and does not have native 2FA capability, so request bank to remove this point. As an alternate as proposed in same point, proposed NDR solution can be integrated with bank's existing MFA solution.	Please refer addendum for the revised clause
2889	49	RFP - Scope of Work 7.3.10 Application security testing Tool	7.3.10.1 Modules, Architecture & Deployment:	Pt 2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Generally AST solutions are deployed with sole purpose of scanning the source code, web, api etc and does not have native 2FA capability, so request bank to remove this point. As an alternate as proposed in same point, proposed AST solution can be integrated with bank's existing MFA solution.	No Change, Please be guided by the RFP
2890	110	RFP - 10.2 Eligibility Evaluation Criteria	OEM Evaluation Criteria	Pt 19. The proposed OEM SIEM Solution with a minimum capacity of 30,000 EPS or 1.2 TB/day shall have been successfully implemented on cloud in one (1) in India.	For wider participation, we request bank to amend the clause as: The proposed OEM SIEM Solution with a minimum capacity of 5,000 EPS or.2 TB/day shall have been successfully implemented on cloud in any one (1) Govt/PSU customer in India. OR The proposed OEM SIEM Solution with a minimum capacity of 10,000 EPS or.4 TB/day shall have been successfully implemented on cloud in one (1) in India.	Please refer addendum for revised clause.
2891	112	RFP - 10.2 Eligibility Evaluation Criteria	OEM Evaluation Criteria	Pt 20. The proposed OEM solution should have been implemented in at least one BFSI is to be submitted for the following solutions: NDR	For wider participation, we request bank to amend the clause as: The proposed OEM solution should have been implemented in at least one BFSI / Govt is to be submitted for the following solutions: NDR	Please refer addendum for the revised clause
2892	260	RFP - 16.21.2 Volumetrics- Solution-wise Requirements	12. Application Security Testing Tool	All the inline components of the solution must operate in high availability mode. In the event of any component failure, the system should automatically initiate failovers within seconds, ensuring uninterrupted functionality without requiring manual intervention.	Application Security Testing as a technology in general works at developemnt/pre-production/UAT stage only. And hence as a solution there is no need of high availability mode. Same has already been updated in this RFP (as solution is asked in standalone at both DC & DR). So, request bank to deleted this clause.	No Change, Please be guided by the RFP. The bidder must design the solution to fully comply with the RFP requirements, ensuring that in case of a failover, the system meets the defined SLA for availability, RTO, and RPO. The bidder is required to adhere to the deployment requirements outlined in the RFP when designing and proposing the solution architecture.
2893	40	APPENDIX 1A Functional Compliance Sheet (Solutions)	Network Detection & Response (NDR)	Pt 8. Proposed solution should generate a root cause analysis, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets.It should provide a platform for easier investigation like visual graphical view and timeline of the attack and it should support tagging of MITRE tactics, techniques and procedures used by the attacker in alerts and incidents.	We reqeust bank to amend the clause: Proposed solution should generate a root cause analysis / incident management, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets.It should provide a platform for easier investigation like visual graphical view and timeline of the attack and it should support tagging of MITRE tactics, techniques and procedures used by the attacker in alerts and incidents.	Please refer addendum for the revised clause
2894	40	APPENDIX 1A Functional Compliance Sheet (Solutions)	Network Detection & Response (NDR)	Pt 13. The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	As bank has asked for on-premise solution for NDR, on the contrary, this clause asks for cloud-native SAAS ask. So, we kindly request bank to delete this clause.	Please refer Addendum for revised clause
2895	42	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 3. The solution must be able to analyse a wide array of programming languages including Java,.Net, C/C++, Objective-C, Android, PHP, COBOL, Ruby, Swift, HTML 5, Scala, APEX, TypeScript, Go, Kotlin and ABAP etc but not limited to these alone	Considering the future requirements of AI in Secure Code Development and most of the development is moving towards AI generated code using AI supported languages. So it is very important for bank to have coverage around this as well and will recommend to incorporate AI supported languages like "R, Ada, Solidity, Bash, Groovy, Rust, Perl", but not limited to these alone.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2896	42	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 24. Solution should support Machine learning and Analysis based on the archived results	ML capability is important, but it is very important to have coverage around AI based code as well. And will recommend bank to consider: The solution should have the capability to scan AI generated code. The solution should be able to integrate with AI coding agent via MCP	No Change, Please be guided by the RFP
2897	43	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 32. The solution should be able to support Composition Analysis: Identify the opens source components used in the application. Vulnerabilities & outdated version Licensing risk associated with the components	Bank is looking for Software composition analysis and asked for identifying the open source component and licensing risk. But this limited information is not enough for bank to secure themselves with rapidly increasing supply chain attacks and we will highly recommend to consider following as well: SCA system must catalogue open source components from Maven, NPM, and Nuget. SCA system has to be able to generate a Bill of Materials for an application. Solution should have the ability to continuously monitor the scanned components & notify if there are any zero day attacks without performing the rescan. Solution should Catalog, Store, and Audit SBOMs (both cycloneDx & SPDX) generated for in-house developed software applications and COTS applications.	No Change, Please be guided by the RFP
2898	30	7.2 Solution & Services Deployment Model and Their HA Requirement 7.2.1 Solutions – Master Deployment Matrix	Sl. No. 8	Vulnerability assessment (VA) & vulnerability lifecycle management Bank Location: Standalone at DC and Standalone at DR. Management Console: Deployed at both DC and DR	Requesting clarifications if standalone management console in DR will be live or will be on standby ?	Please refer addendum for revised clause
2899	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 1 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall be deployable entirely on-premises and shall not require any cloud-hosted component, external service, or Internet connectivity for its core functionality, scanning, management, reporting, analytics, or product capabilities.	Requesting change to: The proposed solution shall be deployable entirely on-premises or hosted on MeitY cloud or Meity empanelled cloud environment. No data shall be shared with the platform/cloud outside India geolocation.	Please refer addendum for the revised clause
2900	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 3 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall be software-based and fully deployable on the hardware infrastructure proposed by the Bidder.	Requesting change to: The proposed solution shall be software-based and fully deployable on the hardware infrastructure or should support hybrid- on-premise architecture with management-console or scanners on on-premise and analytics components on MeitY/MeitY-emapanneled cloud proposed by the Bidder.	No Change, Please be guided by the RFP
2901	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 9 of Vulnerability Assessment & vulnerability lifecycle Management	Each scanning engine shall support web application security assessment together with traditional infrastructure vulnerability and configuration/compliance assessment. The solution shall identify vulnerabilities, missing patches, insecure configurations, and compliance deviations, and generate comprehensive reports containing risk severity, evidence of findings, affected assets, and remediation recommendations to support security governance, audit, and regulatory compliance.	Requesting to confirm that if DAST specs are specifically provided for web-application's VAPT, then what is the scope of "web-application" scanning in this spec? Also requesting to share the total number of web-applications considered in the scanning scope.	No Change, Please be guided by the RFP
2902	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 18 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall support both active and passive asset discovery and vulnerability assessment/scanning.	Requesting change to: The proposed solution shall support both active and/or passive asset discovery and vulnerability assessment/scanning.	No Change, Please be guided by the RFP
2903	48	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 27 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall support both active and passive techniques for vulnerability detection, where applicable.	Requesting change to: The proposed solution shall support both active and/or passive techniques for vulnerability detection, where applicable.	No Change, Please be guided by the RFP
2904	48	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 33 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall support deployment and lifecycle management of scanning agents without dependency on cloud-hosted services.	Requesting change to: The proposed solution shall support deployment and lifecycle management of scanning agents.	No Change, Please be guided by the RFP
2905	48	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 34 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall assess Active Directory security posture and identify misconfigurations, privilege risks, insecure policies, and exposure of critical directory services.	Requesting to clarify that this spec is already addressed in IDTR then what is the requirement of it in VM solutin?	No Change, Please be guided by the RFP
2906	49	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 74 of Vulnerability Assessment & vulnerability lifecycle Management	The solution shall support offline signature and plugin updates for deployment in isolated or air-gapped environments.	Requesitng to remove this spec because if the cloud-based solution is offered and where cloud is hosted on MeitY cloud or MeitY empanneled cloud then questions related to air-gap environment doesn't arise.	No Change, Please be guided by the RFP
2907	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 81 of Vulnerability Assessment & vulnerability lifecycle Management	The solution shall support password-protected and/or digitally signed reports with configurable retention and archival.	Requesting change to: The solution must support secure, encrypted report distribution (including native PGP encryption) and enforce strict role-based access controls (RBAC) for report viewing. Additionally, the platform must provide configurable cloud-based data retention policies alongside automated options to archive historical scan data and reports to external storage	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2908	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 87 of Vulnerability Assessment & vulnerability lifecycle Management	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	Requesting change to: The solution must provide AI-generated risk summaries and plain-language vulnerability briefs that automatically fuse asset criticality, technical findings, and real-world threat telemetry (such as CISA KEV and EPSS data) to streamline IT triage. If cloud analytics are utilized to run these machine learning models, the solution vendor must guarantee that all data is isolated within dedicated, bank-authorized cloud regions, employing strict data privacy frameworks that ensure source code, credentials, and raw scan parameters are explicitly excluded from public AI training models or multi-tenant public AI services	Please refer addendum for revised clause
2909	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 88 of Vulnerability Assessment & vulnerability lifecycle Management	Unified, correlated findings intelligence. Every scanning engine — across web, API, network and host, cloud, containers, mobile, source code, device configuration and identity — reports into a single normalized findings model..	Requesting clarification on why unified reporting is asked as the ASM, VM, DAST solutions are considered separately.	No Change, Please be guided by the RFP
2910	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 90 of Vulnerability Assessment & vulnerability lifecycle Management	Mobile Application Security Testing: The proposed solution shall support static security analysis of Android and iOS mobile application packages, including APK/AAB and IPA formats, and shall provide security assessment mapped to recognized mobile application security standards and methodologies such as OWASP MASVS and MASTG.	Requesting clarification for the spec as the ask is for DAST or MAST solution.	No Change, Please be guided by the RFP
2911	87	Anti Phishing Services	17.1	Solution should detect at the earliest point in the attack, post initial compromise as the attacker is first attempting to move laterally and escalate privilege.	Since this section is focused on Anti-Phishing, we understand that the objective is to identify suspicious activity following a successful phishing or account-compromise event. Network-level lateral movement and deception capabilities may be addressed by other security controls. We request the Bank to clarify whether this clause may instead focus on early post-compromise user activity visibility for the Bank's most critical users. " The solution should support early identification and investigation of suspicious user activities associated with potential account compromise following phishing or other email-originated attacks, with enhanced user activity monitoring for up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles."	Please refer to the relevant Addendum for updated specfications
2912	87	Anti Phishing Services	17.4	Solution must provide robust supply chain and AI/ML-driven contact chain analysis capabilities to identify and defend against socially engineered, impersonated, or BEC attacks.	As compromise of trusted suppliers and partners is an important source of BEC and phishing risk, we request the Bank to clarify whether the existing supply-chain requirement should explicitly include behavioural analysis of supplier/partner communication patterns to identify attacks originating from compromised trusted accounts. " Solution must provide robust supply-chain and AI/ML-driven contact-chain and behavioural analysis capabilities to identify and defend against socially engineered, impersonated or BEC attacks, including threats originating from compromised or impersonated supplier/partner accounts."	Please refer to the relevant Addendum for updated specfications
2913	87	Anti Phishing Services	18	Solution must proactively analyze suspicious URLs using dynamic/behavioral analysis to prevent the spread of malware and other threats.	The RFP separately addresses URL analysis and post-delivery remediation. We request clarification whether these requirements are intended to provide continuous protection throughout the email threat lifecycle, including pre-delivery analysis, click-time URL protection and post-delivery detection/remediation. " Solution must provide continuous protection across the email threat lifecycle, including pre-delivery threat detection, real-time/click-time inspection of suspicious URLs, and post-delivery detection and automated remediation of threats that are subsequently determined to be malicious."	Please refer to the relevant Addendum for updated specfications
2914	88	Anti Phishing Services	19.7	Solution must be able to offer a comprehensive portal that allows users to access information and metadata on events/incidents, facilitating network threat forensics for thorough investigation and analysis of potential security breaches or incidents.	To strengthen investigation of phishing-led incidents involving executives and other critical users, we request clarification whether the existing forensic portal requirement may also include contextual user and endpoint activity for a limited population of Bank-identified critical/high-risk users. " Solution must offer a comprehensive investigation portal providing information and metadata on events/incidents for forensic analysis. For up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, the portal should additionally provide contextual user and endpoint activity, including relevant application, file and user-action details, to support investigation of potential phishing-led compromise."	Please refer to the relevant Addendum for updated specfications
2915	88	Anti Phishing Services	19.9	Solution must empower security operations and incident responders to automate the identification, remediation, and sharing of phishing threats, streamlining the process of detecting, addressing, and disseminating information about potential phishing attacks for improved response and mitigation.	To improve SOC investigation efficiency, we request clarification whether the existing phishing identification and remediation requirement should include centralized attack context showing why a message was identified as malicious, the users targeted, associated threat indicators and remediation status. " Solution must empower security operations and incident responders to automate identification, investigation, remediation and sharing of phishing threats, and should provide centralized contextual visibility into the users targeted, associated threat indicators, detection rationale, attack characteristics and remediation actions."	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2916	88	Anti Phishing Services	19.1	Solution must provide incident responders with real-time analytics and visibility into email-based attacks targeting the organization.	Email-based attacks against executives and privileged users may require additional context after delivery to determine whether a targeted user has subsequently performed suspicious activity. We request the Bank to clarify whether real-time investigation visibility may include relevant user activity context for up to 100 Bank-identified critical/high-risk users. " Solution must provide incident responders with real-time analytics and visibility into email-based attacks targeting the organization. For up to 100 Bank-identified critical/high-risk users, the solution should additionally provide contextual visibility into suspicious user activities associated with potential phishing or account compromise, including relevant user, endpoint, application and file activity."	Please refer to the relevant Addendum for updated specfications
2917	88	Anti Phishing Services	19.23	Solution must have simplicity of evaluation and additional visibility into internal traffic and other communication channels can reduce risk, and baseline user activity to detect suspicious behavior.	The existing clause already seeks baselining of user activity to detect suspicious behaviour. We request the Bank to clarify the intended depth and scope of this capability and whether enhanced monitoring may be applied to a focused population of up to 100 Bank-identified critical/high-risk users, where deeper visibility provides the greatest security value. " Solution must provide additional visibility into relevant internal activity and communication channels to reduce risk and baseline user activity to detect suspicious behaviour. Enhanced user and data activity monitoring should be provided for up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, with configurable detection policies for suspicious, anomalous or policy-violating activities."	Please refer to the relevant Addendum for updated specfications
2918	90	Anti Phishing Services	19.7	Solution must provide protection against harassment mail and mitigate the risks associated with emails from unknown senders specifically for executives or VIPs, safeguarding them from potential threats and ensuring their email communication remains secure.	Since this clause already provides enhanced protection for executives/VIPs, we request the Bank to clarify whether such enhanced protection should extend beyond receipt of suspicious email to investigation of risky user and data activities that may occur following phishing or account compromise, for a limited set of the Bank's most critical users. "Solution must provide protection against harassment mail and mitigate risks associated with emails from unknown senders specifically for executives or VIPs. For up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, the solution should additionally provide enhanced visibility into risky user and data activities following suspected phishing or account compromise, including relevant file movement, web/upload activity, removable-media activity and other supported data-transfer channels."	Please refer to the relevant Addendum for updated specfications
2919	52	Idendity Threat Detection and Response (ITDR)	1.7	Detect and respond to active threats with high fidelity (low false positives and false negatives).	The Bank has separately specified a comprehensive deception platform for detection of active attacker activity, reconnaissance and lateral movement. We understand that the intent of this clause within ITDR is therefore to complement those controls with focused monitoring of the Bank's most critical identities. Considering that enhanced user-activity monitoring is most relevant for high-risk personnel such as executives, privileged users and other critical users, we request the Bank to kindly clarify whether this requirement may be read as follows: " Identity Threat Detection Solution should provide high-fidelity detection and response for risky or anomalous user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, to identify activities associated with careless, malicious or compromised users. "	No Change, Please be guided by the RFP
2920	52	Idendity Threat Detection and Response (ITDR)	1.8	Provide contextual information—who, what, when and how—to inform all stages of the attack chain.	The Bank has already sought attack-lifecycle visibility under the separate deception requirements. For ITDR, we understand that additional value would be derived from detailed user-centric context for the Bank's most critical identities, enabling investigation of risky activity performed by such users. We request the Bank to kindly clarify whether this requirement may be read as follows: " Identity Threat Detection Solution should provide contextual information—who, what, when, where and how—around risky user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, to support investigation and response."	No Change, Please be guided by the RFP
2921	52	Idendity Threat Detection and Response (ITDR)	1.9	Provide deep insights into both the potential and used privilege escalation and lateral movement steps in an attack.	Privilege escalation and lateral-movement visibility is already substantially addressed under the separately specified deception solution, including attacker lifecycle visibility, MITRE ATT&CK mapping, deceptive attack paths and detection of lateral movement. To avoid duplication while retaining complementary investigation capability for high-risk identities, we request the Bank to kindly clarify whether this requirement may be read as follows: "Identity Threat Detection Solution should provide deep insights into activities performed by up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, covering application usage, file and data movement, endpoint activity and other risky behaviours to support investigation of compromised, malicious or negligent user activity."	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2922	52	Idendity Threat Detection and Response (ITDR)	2.9	Detect all types of attack vectors including pre-attack reconnaissance, zero-day attacks, privilege escalation prevention, lateral movement and data theft.	Pre-attack reconnaissance, lateral movement, malware/attack behaviour and attacker lifecycle visibility are already covered under the Bank's separate deception specifications. We understand that the complementary requirement under ITDR should focus on identity/user risk and potential data-loss activity for the Bank's most critical users rather than duplicate the deception control. We request the Bank to kindly clarify whether this requirement may be read as follows: " Identity Threat Detection Solution should detect risky user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, including suspicious application usage, unauthorized access or movement of sensitive information, removable-media activity, web-based transfer, cloud synchronization and other potential data-exfiltration activities."	The Clause is applicable only to idendity related threat vector only. The volumetrics is provided in the RFP and should be complied
2923	52	Idendity Threat Detection and Response (ITDR)	2.10	Detect multiple attacks simultaneously.	We understand the intent is to ensure that the solution is not restricted to investigation of a single event at a time. Since active attacker detection is separately covered by the deception solution, we request that this clause be clarified in terms of concurrent monitoring and investigation of risky activities across the Bank's designated critical-user population: "Identity Threat Detection Solution should be capable of detecting and investigating multiple risky user and data activities simultaneously across up to 100 critical/high-risk users and their monitored endpoints."	No Change, Please be guided by the RFP
2924	52	Idendity Threat Detection and Response (ITDR)	3.2	Provide unified presentation of both source- and target-based telemetry data in a timeline view.	The Bank has separately specified end-to-end attacker visibility and behavioural analysis under the deception solution. For ITDR investigations involving critical identities, a chronological user-activity view would provide complementary evidence of actions performed by the user. We request the Bank to kindly clarify whether the requirement may be read as follows: " Identity Threat Detection Solution should provide a unified chronological timeline of user- and endpoint-based activity telemetry for up to 100 critical/high-risk users identified by the Bank to support investigation of risky or suspicious user activity."	No Change, Please be guided by the RFP
2925	52	Idendity Threat Detection and Response (ITDR)	3.3	Correlate identity-related telemetry from relevant source and target systems to identify and investigate identity compromise, privilege escalation, credential abuse and lateral movement.	Privilege escalation and lateral-movement detection are already addressed through the separately specified deception controls. To provide complementary investigation capability for the Bank's highest-risk identities, we request the Bank to clarify whether this clause may focus on correlation of user, endpoint, application and data activity for the designated critical-user population: " The solution shall support correlation of user, endpoint, application and data-activity telemetry for up to 100 critical/high-risk users identified by the Bank to identify and investigate suspicious user behaviour, sensitive-data movement, policy violations and potential data-exfiltration activities."	No Change, Please be guided by the RFP
2926	52	Idendity Threat Detection and Response (ITDR)	3.4	Integrate with compatible endpoint/extended detection solution to capture screen recordings or screenshots during active attacker sessions as advanced forensic evidence.	The Bank has separately specified attacker-session and forensic visibility through the deception platform. Within ITDR, we understand that visual evidence is intended to strengthen investigation of high-risk user activity. We request the Bank to kindly clarify whether the requirement may be read in an outcome-based manner for the designated critical-user population: " The Identity Threat Detection Solution should support screenshots, screen capture or equivalent visual evidence of relevant activity for up to 100 critical/high-risk users during suspicious or high-risk user sessions, as part of forensic investigation and evidence collection."	Please refer addendum for revised clause.
2927	52	Idendity Threat Detection and Response (ITDR)	3.5	Integrate with compatible network detection solution to support collection of PCAP data for network-level incident visibility.	The requirement for PCAP is network-centric and does not directly relate to identity posture or focused user-activity monitoring. Further, the Bank's separate deception specifications already require high-interaction decoys, recording of attacker activities, traffic/behaviour visibility, forensic investigation and integration with network/security technologies. To avoid duplication of network-level forensic controls across two solution categories, we request the Bank to kindly delete this clause from the ITDR section.	Please refer addendum for revised clause.
2928	52	Idendity Threat Detection and Response (ITDR)	3.6	Push incident data into SIEM/XDR or SOAR technologies via integrations for improved incident management.	We understand that the objective is to ensure relevant ITDR alerts and investigation context are available to the Bank's SOC ecosystem. For the enhanced monitoring of designated critical users, we request the Bank to kindly clarify whether alerts and activity information may be shared through supported integrations or APIs as follows: " Identity Threat Detection Solution should make alerts and relevant incident/activity data for the monitored critical-user population available to SIEM/XDR, SOAR or other supported security platforms through integrations or APIs for improved incident management."	The proposed solution hould be integrated with SIEM/XDR or SOAR technologies for sharing the incident data via supported integrattion or APIs
2929	52	Idendity Threat Detection and Response (ITDR)	3.7	As part of forensic data collection, include detailed attack path information including protocols leveraged during the attack.	Detailed attack-path and attacker-behaviour visibility is already sought under the separate deception specifications, including deceptive attack paths, MITRE ATT&CK mapping and forensic investigation. To avoid overlap while retaining complementary evidence for investigations involving the Bank's critical identities, we request the Bank to kindly clarify whether the requirement may be read as follows: " Identity Threat Detection Solution should, as part of forensic data collection for up to 100 critical/high-risk users, include detailed user-activity information such as applications used, files accessed, data movement, destination channels and other relevant endpoint activity associated with the incident."	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2930	52	Idendity Threat Detection and Response (ITDR)	3.8	Collect user and computer information from Active Directory as part of forensic data gathering to enhance context and assess risk exposure.	We understand that directory information is required to enrich investigations with user and computer context. We request the Bank to clarify that enterprise identity context may be maintained for the overall identity population, while detailed endpoint/user-activity telemetry may be applied to the Bank's designated critical-user population: " Identity Threat Detection Solution should use relevant user and computer identity information to enhance forensic context and risk assessment, and should correlate such context with detailed endpoint/user-activity telemetry for up to 100 critical/high-risk users identified by the Bank."	Please refer addendum for revised clause
2931	52	Idendity Threat Detection and Response (ITDR)	3.9	Detect an adversary's attempt to move laterally toward key assets using as many Windows, Mac or Linux hosts as possible without requiring a persistent agent.	The Bank's separate deception specifications expressly require detection of lateral movement, reconnaissance, credential theft and malicious activity using agentless and/or agent-based deception techniques across the enterprise. The present clause therefore duplicates a capability already being procured under the Deception section. To avoid overlapping scope and duplicate controls, we request the Bank to kindly delete this clause from the ITDR section.	Please refer addendum for revised clause
2932	52	Idendity Threat Detection and Response (ITDR)	3.10	Collect AD user/computer information for forensic context and detect at the earliest point post initial compromise as the attacker first attempts lateral movement and privilege escalation.	Early detection of lateral movement and privilege-escalation activity is substantially covered under the Bank's separate deception requirements. To retain a complementary identity/user-risk objective without duplicating the deception scope, we request the Bank to kindly clarify whether this clause may focus on early detection of risky activity among the designated critical-user population: " Identity Threat Detection Solution should use relevant identity context and detect risky user behaviour at the earliest possible point for up to 100 critical/high-risk users, based on monitored endpoint activities and configured detection policies, enabling investigation and response before such activity results in significant data loss or business impact."	Please refer addendum for revised clause
2933	52	Idendity Threat Detection and Response (ITDR)	3.11	Collect AD user/computer data during forensic gathering while ensuring all deception techniques remain hidden from legitimate users.	The requirement to ensure deception techniques remain hidden from legitimate users is inherently a deception-platform capability. The Bank has already included comprehensive deception requirements covering lures, breadcrumbs, fake credentials, deceptive assets, attacker engagement and techniques designed to remain undetected by attackers. We therefore request the Bank to kindly delete this clause from the ITDR section to avoid duplication.	Please refer addendum for revised clause.
2934	2	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	10	OEM shall ensure compliance of the complete proposed solution & platform with RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and all applicable regulations throughout the contract period.	We request the Bank to clarify that the OEM is required to maintain applicable security, privacy and regulatory controls relevant to the services provided and furnish available compliance/assurance documentation, while the overall regulatory compliance obligation of the Bank remains subject to the Bank's deployment, configuration and usage of the service. " OEM shall maintain security, privacy and compliance controls applicable to the proposed hosted service and shall provide available independent assurance reports, certifications and relevant compliance documentation to support the Bank's obligations under applicable RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and other applicable regulatory requirements."	Please refer addendum for revised clause
2935	2	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	20	The Service uptime agreement for the proposed solution on cloud should have monthly uptime commitments and have transparent monthly credit calculations in case of uptime not being met for any services.	We understand that published/contracted OEM hosted-service SLA commitments and corresponding service-credit methodology shall meet this requirement. Kindly confirm.	No Change, Please be guided by the RFP
2936	3	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	29	Solution provider should provide the design and process for data deletion in the scope of an independent audit and that the operational effectiveness of these controls is tested. The report for the same should be submitted to bank as and when asked by bank.	For a globally operated hosted security service, control effectiveness is generally evidenced through independent assurance reports such as SOC 2 Type II and documented data-retention/deletion controls. We request the Bank to permit such independent assurance documentation instead of requiring a separate bespoke data-deletion audit report. " Solution provider shall maintain documented secure data-retention and deletion controls. Compliance may be demonstrated through applicable independent third-party assurance reports/certifications (such as SOC 2 Type II or equivalent) and documented data-retention/deletion policies made available subject to OEM confidentiality requirements."	Please refer addendum for the revised clause
2937	4	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	41.3	Independent audit for testing effectiveness of secure data removal, such that data is rendered permanently inaccessible. (Including any backup or distributed online media).	We request the Bank to accept independently audited secure deletion and media-management controls, together with documented retention/deletion periods, rather than requiring a customer-specific audit of all backup and distributed media. " The OEM shall maintain secure data deletion, media handling and backup-retention controls designed to render customer data inaccessible in accordance with documented retention schedules. Effectiveness may be evidenced through independent assurance reports such as SOC 2 Type II/ISO 27001 or equivalent and relevant OEM security/privacy documentation."	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2938	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	47.2	Bank shall have an option to implement 'Bring Your Own Key' as and when required.	The proposed service protects data at rest and in transit using strong encryption; however, customer-managed infrastructure encryption keys are not a standard capability of the hosted anti phishing service. We request deletion of the BYOK requirement, or acceptance of OEM-managed enterprise-grade encryption and key-management controls. " Requested Action: Delete the BYOK requirement. Alternatively: 'Data processed/stored by the hosted service shall be protected using industry-standard encryption in transit and at rest, with secure OEM-managed key-management controls subject to independent security assurance.'"	Please refer addendum for the revised clause
2939	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	49	Web Application Firewall shall be implemented on the cloud for Web based applications. WAF application signature should be updated and reviewed regularly. The Report shall be submitted to bank on a periodic interval.	Since the proposed platform is an OEM-managed hosted security service, underlying WAF technology, signatures and configurations form part of the OEM's internal security architecture and may not be exposed as customer-specific reports. We request the Bank to accept periodic VAPT/penetration-test assurance or equivalent independent security assessment evidence covering the hosted application instead of WAF signature reports. " The hosted web application/platform shall be protected through appropriate application-security controls. The OEM shall conduct periodic vulnerability assessment and penetration testing/security assessments and, subject to confidentiality restrictions, provide an executive summary/attestation or applicable independent assurance evidence to the Bank on request. Customer-specific WAF signature reports shall not be mandatory."	Please refer addendum for revised clause
2940	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	52	The systems in cloud infrastructure should be periodically updated with the latest anti-malware signatures, the bidder shall submit the periodic report on the same with bank.	For an OEM-managed hosted security service, infrastructure anti-malware/endpoint controls are centrally managed and independently audited. We request the Bank to accept OEM security assurance and vulnerability/malware-control attestations rather than periodic host-level signature reports. " The OEM shall maintain appropriate malware protection, vulnerability management, patching and security monitoring controls for the hosted infrastructure. Compliance may be evidenced through independent assurance reports/certifications and applicable security-control attestations instead of customer-specific anti-malware signature update reports."	Please refer addendum for revised clause
2941	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	53	Data Loss Governance and risk management framework shall be defined by bidder for workload on the cloud and same shall be shared with bank on periodic basis. Data loss prevention controls should be implemented to secure the data in the cloud environment from unauthorized or inadvertent exfiltration.	We request clarification that the requirement is intended to ensure protection against unauthorized/inadvertent data exfiltration through the proposed service and appropriate security controls for hosted customer data, rather than requiring disclosure of the OEM's internal cloud governance framework. " The proposed solution shall provide configurable controls to identify and prevent unauthorized or inadvertent transmission/exfiltration of sensitive information through any channels. The OEM shall maintain appropriate access control, encryption and data-protection controls for customer data processed within the hosted service and provide applicable assurance documentation on request."	Please refer addendum for revised clause
2942	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	81	Log generation, storage and review process should be certified by CERT IN empaneled auditor, report for the same shall be submitted by bidder as and when required by bank.	For global SaaS/POD services, security logging and monitoring controls are typically independently audited under recognized assurance frameworks. We request the Bank to accept SOC 2 Type II/ISO 27001 or equivalent independent assurance in lieu of a mandatory CERT-In-empanelled audit of the OEM's internal log-generation/storage/review process. " The OEM shall maintain documented security logging, monitoring, retention and review controls. Effectiveness shall be evidenced through applicable independent third-party assurance reports/certifications such as SOC 2 Type II, ISO 27001 or equivalent. CERT-In-empanelled audit may be required only for bidder-managed components deployed specifically within the Bank environment, where applicable."	Please refer addendum for the revised clause
2943	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	82.5	IT Act 2000 & its amendments, and other Acts/Regulatory guidelines.	Kindly clarify that the OEM must comply with legal/regulatory requirements applicable to it as the provider of the proposed hosted service and provide reasonable documentation to support the Bank's compliance obligations. " OEM shall comply with applicable legal and regulatory obligations relevant to its provision of the proposed service and shall provide available security/privacy/compliance documentation reasonably required to support the Bank's applicable obligations."	Please refer addendum for the revised clause
2944	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	83	CERT IN Empaneled auditor report's is required for the following:	We request the Bank to permit internationally recognized independent assurance reports/certifications for OEM-managed hosted services. CERT-In empanelled audit reports may remain applicable to India-specific bidder-managed/on-premises components where such audit is feasible and required. " For OEM-managed hosted/SaaS services, independent assurance reports/certifications such as SOC 2 Type II, ISO 27001 or equivalent shall be accepted. CERT-In empanelled audit reports shall be applicable only to components/services for which such India-specific audit is contractually and technically feasible."	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2945	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	92	The application and DB is/will be hosted separately on a dedicated infrastructure (physical/logical) for PSB. Evidence of dedicated infrastructure (physical/logical) for PSB should be submitted.	The proposed platform is an OEM-managed hosted security service designed with logical access controls and customer data isolation. Requiring dedicated physical application/database infrastructure would restrict standard SaaS/POD architectures without necessarily improving the security outcome. We request acceptance of secure logical tenant/customer isolation supported by independent assurance evidence. " The proposed hosted service shall provide secure logical segregation/isolation of Bank data and administrative access from other customers through appropriate access-control and tenant-isolation mechanisms. Dedicated physical application/database infrastructure shall not be mandatory where equivalent logical isolation is implemented and independently assured."	Please refer addendum for the revised clause
2946	8	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	98.1	Feasibility to audit/review IT controls of the third party or obtaining independent review report for the same from CERT-In empaneled security consultant, to ensure it meets Bank's information security requirement.	We request that the Bank permit review of current independent assurance reports/certifications as the primary mechanism for reviewing OEM IT controls. Any direct audit should remain subject to the OEM's standard contractual audit provisions, confidentiality, security, scope and advance-notice requirements." The Bank may review applicable independent third-party assurance reports/certifications covering the hosted service. Where additional audit is required, such audit shall be subject to mutually agreed scope, confidentiality/security restrictions, reasonable advance notice and the OEM's standard contractual audit provisions. A CERT-In empanelled consultant may review evidence made available under these conditions."	Please refer addendum for the revised clause
2947	30, 34	7.2.1 Deployment Model & HA (TIP) / 7.2.4.1 Deployment Pattern	Table 7.2.1 Sr. 7; Cl. 7.2.4.1(e)	"Threat Intelligence Platform (TIP) - Cloud (SaaS) + Hybrid - Bank Location: Broker/Collector/Integrator: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR" (Table 7.2.1).	Cyble's Threat Intelligence Platform (TIP) is delivered as a fully cloud-native SaaS solution, providing continuous threat-intelligence aggregation, enrichment and distribution to the Bank via API, STIX/TAXII feed and a dedicated web portal, with high availability, geographic resiliency and disaster recovery built into the SaaS platform itself - fully aligned with the SLA, RTO and RPO defined in Section 13. As the TIP's core function requires no packet-level or in-line processing within the Bank's network, Cyble can meet the Bank's continuity requirement for this solution without deploying a broker/collector component on Bank premises. We request the Bank's confirmation that this cloud-native delivery model will be accepted as fully compliant with Table 7.2.1.	Please refer addendum for the revised deployment requirement
2948	55-56	7.4.3 Attack Surface Management	Cl. 7.4.3	"Discovery of internet-facing and internal assets... The proposed solution shall provide AI-enabled Attack Surface Management (ASM) capabilities for continuous discovery... of the organization's external attack surface, including known and unknown internet-facing assets."	Cyble's Attack Surface Management (ASM) capability provides continuous, AI-enabled discovery, monitoring and risk-prioritization of the Bank's entire external attack surface - internet-facing assets, exposed services, domains, cloud assets and shadow IT - using external/passive reconnaissance together with Bank-shared asset inventories (IP ranges, domains, cloud accounts), with no agent or appliance required inside the Bank's network, consistent with the offsite Managed Service model in Section 7.2.2. This gives the Bank a complete outside-in exposure view from Day 1. We request the Bank's confirmation that this externally-led, agentless approach satisfies Cl. 7.4.3.	Bank is looking for external attack surface management
2949	57	7.4.6 Dark Web Monitoring	Cl. 7.4.6	"...offsite, tool-based continuous dark web and cyber threat exposure monitoring services... across the surface web, deep web, dark web, underground forums, messaging platforms, and data leak repositories."	Cyble's Dark Web & Cybercrime Monitoring capability continuously covers the surface web, deep web, dark web, underground forums, messaging platforms and data-leak repositories, and can begin protecting the Bank's specified identities, brand keywords and domains immediately upon contract signature. To tailor this coverage precisely, we request the Bank share the initial monitoring scope (employee/executive identities, brand keywords, domains and relevant data categories) so Cyble can confirm sizing and reporting cadence.	Details shall be shared with succesful bidder
2950	57	7.4.7 Threat Intelligence Feed	Cl. 7.4.7(l)	"Provision of threat intelligence through a centralized portal/dashboard and/or machine-readable feeds."	Cyble's Threat Intelligence Feed is delivered through both a centralized portal/dashboard and machine-readable, standards-based feeds (STIX/TAXII, MISP-compatible formats and API), enabling seamless integration with the Bank's existing or future security stack whenever required. We confirm this dual delivery model - portal-based consumption plus machine-readable feed/API - and request the Bank's confirmation that it satisfies Cl. 7.4.7.	No Change, Please be guided by the RFP
2951	57-58	7.4.8 Threat Hunting Services	Cl. 7.4.8(m)	"The threat hunting service shall be delivered remotely/offsite using secure and mutually agreed mechanisms for accessing relevant logs, telemetry, security tools, and data made available by the Bank."	Cyble can deliver proactive, intelligence-driven Threat Hunting entirely offsite - correlating curated external threat intelligence (IOCs, IOAs, TTPs, threat-actor and campaign intelligence) against Bank-shared context, supplemented by secure, mutually agreed read-only access to relevant Bank telemetry for validation and deeper investigation as needed - fully consistent with the remote/offsite delivery model mandated in Cl. 7.4.8(m). We request the Bank's confirmation that this intelligence-led hunting model, combined with agreed read-only telemetry access, meets the Bank's requirement.	No Change, Please be guided by the RFP
2952	58	7.4.9 Brand Protection and Monitoring	Cl. 7.4.9(j)	"Takedown coordination with relevant registrars, hosting providers, platforms, application stores, social media platforms, and other relevant entities, wherever applicable."	Cyble's Brand Reputation Monitoring capability continuously identifies brand impersonation, typosquatting, phishing/fraudulent websites, fraudulent mobile apps and social-media impersonation, and actively coordinates takedown requests with registrars, hosting providers, app stores and social platforms on the Bank's behalf under a standard authorisation executed at contract signature - delivering a fully managed, end-to-end takedown process with minimal effort required from the Bank's team. We request the Bank's confirmation that this bidder-led takedown coordination model satisfies Cl. 7.4.9(j).	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2953	256	16.21 Annexure 21: Sizing/Volumetrics (gap for Offsite Services)	Annexure 21, Sizing table	Annexure 21's sizing table provides explicit volumetrics (EPS, endpoint counts, IPs, VPCs, etc.) for the 14 solutions under Section 7.3, but no equivalent executive/VIP count is specified for the offsite services that monitor executive exposure (Anti-Phishing - Cl. 7.4.5, Dark Web Monitoring - Cl. 7.4.6, Brand Protection - Cl. 7.4.9).	Cyble's Executive Monitoring and Digital Risk Protection capabilities can protect any number of the Bank's executives/VIPs from Day 1, with coverage scaled precisely to the Bank's requirement across Anti-Phishing, Dark Web Monitoring and Brand Protection. To finalise sizing, we request the Bank confirm the number of executives/VIPs (e.g., Board members, CXOs, senior management) to be brought under continuous monitoring at contract commencement.	Please refer to the relevant Addendum for updated specfications
2954	54	7.4 Functional Requirement - Services (Offsite Services)	Cl. 7.4(d)	"The Bidder shall implement appropriate security controls, including data masking or tokenization for sensitive data, Role-Based Access Control (RBAC), Just-in-Time (JIT) privileged access, and comprehensive audit logging for all services delivered under this RFP." - no named-user/license count is specified for platform/dashboard access to the 9 offsite services.	Cyble's platform can be provisioned for any number of the Bank's analysts, CISO-office and compliance stakeholders who need dashboard access to the offsite services, with full role-based access control as required under Cl. 7.4(d). To size the commercial bid precisely, we request the Bank confirm the number of named analyst/console user licenses required for the Bank's teams to access Cyble's platform and reporting for the proposed offsite services.	details shall be shared with successful bidder
2955	259	16.21.2 – Volumetrics – Solution-wise Requirements	UEBA – Item 7	UEBA: Total 50,000 sustainable EPS / 2.06 TB per day, scalable to 75,000 EPS / 3.09 TB per day; 12,000 Endpoint Users scalable to 16,000.	Please clarify the total number of user identities to be monitored by UEBA (employees, contractors, privileged users, service accounts, etc.). Also confirm whether the stated 12,000/16,000 figure represents endpoint users, unique identities, or both.	Please refer addendum for the revised clause
2956	39–40	7.3.1 – Security Information and Event Management	7.3.1.1, Clauses 5–6	SIEM shall integrate with the Bank's entire IT ecosystem and collect logs/telemetry from servers, endpoints, network devices, security appliances, databases, applications, access management, cloud, SaaS/PaaS/IaaS, containers, APIs and third-party systems.	Please provide the list of major data source types to be integrated with SIEM/UEBA, together with the approximate count of instances/devices for each source type.	ITSM - Manage Engine
2957	26, 34–35	7.1 / 7.2.4 – Scope & Deployment Architecture	7.1; 7.2.4.1	The solution shall cover the Bank's DC, DR, cloud environments and branches, using a hybrid model with Cloud/SaaS and Bank-hosted components.	Please share the Bank's current cloud footprint (AWS/Azure/GCP/other), key cloud services in use, and the expected cloud expansion roadmap during the contract period.	Details shall be shared with successful bidder
2958	34–36	7.2.4 – Deployment Architecture	7.2.4 / 7.2.4.2	Bank-hosted collectors/brokers/sensors/connectors shall exchange telemetry securely with Cloud/SaaS platforms across DC, DR, branches and cloud environments.	Please clarify how the in-scope data sources are distributed across DC, DR, branches, cloud accounts/subscriptions, regions and other locations, including any major network segmentation or restricted connectivity zones.	Details shall be discussed with succesfull bidder
2959	26, 28, 67	7.1 / 7.6.8 – Compliance & Security Requirements	7.1; 7.6.8, Clause 5	The proposed solution shall support compliance with RBI, CERT-In, DPDP Act, Government of India requirements, Bank policies and other applicable regulations/standards.	Please confirm the compliance and regulatory frameworks that must be specifically addressed through SIEM, UEBA, SOAR and TIP reporting/use cases, including any Bank-specific policies or audit requirements.	No Change, Please be guided by the RFP
2960	36	7.2.4.2 – Connectivity and Data Flow	7.2.4.2	Telemetry sources include users, endpoints, servers, applications, databases, network devices, IoT/OT systems, cloud services and other sources.	Please confirm whether OT/ICS telemetry is in scope. If yes, please share the OT security platform(s) currently deployed (e.g., Claroty, Nozomi), approximate number of OT assets, and whether OT and IT environments are located in the same or separate network/DC zones.	No Change, Please be guided by the RFP, further details shall be shared with the successful bidder
2961	42	7.3.2 – SOAR	7.3.2.2, Clause 2	SOAR shall integrate with SIEM, XDR, NDR, UEBA, TIP, ITSM, IAM/PAM, network, endpoint, cloud and other relevant security solutions.	Please confirm the ITSM platform to be integrated for automated ticket/case creation and updates (e.g., ServiceNow, BMC, Jira, ManageEngine), including any specific workflow or bi-directional integration requirements.	ITSM - Manage Engine
2962	42	7.3.2 – SOAR	7.3.2.2, Clauses 2–4	SOAR requires integrations and development/customization of response workflows/playbooks for enrichment, investigation, containment, remediation and response verification.	Please provide the list of security and IT technologies that are expected to be integrated with SOAR for automated enrichment and response actions.	Details shall be shared with successful bidder
2963	45–46	7.3.7 – Threat Intelligence Platform	7.3.7.1, Clauses 3–10	TIP shall aggregate, normalize, score, contextualize and manage threat intelligence from multiple sources and use validated intelligence in automation/response workflows.	Please confirm whether the Bank currently subscribes to any commercial or sector-specific threat intelligence feeds that must be integrated with TIP/SOAR. If yes, please provide the feed/provider names and integration method, where available.	Details shall be shared with successful bidder
2964	42	7.3.2 – SOAR	7.3.2.2, Clauses 3–4	The bidder shall develop, customize, test, tune and maintain response workflows/playbooks, including automated enrichment, investigation, containment and remediation.	Please share the top five priority SOAR playbooks/use cases expected to be implemented during the initial phase, along with any mandatory approval/exception controls.	No Change, Please be guided by the RFP
2965	46	7.3.7 – Threat Intelligence Platform	7.3.7.1 / 7.3.7.2	TIP shall collect intelligence from multiple sources and support IOC/IOA/TTP lifecycle management, scoring, enrichment, curation and dissemination.	Please provide the list of existing commercial, open-source, government/CERT-In, ISAC or other threat intelligence feeds/sources that are expected to be integrated with the proposed TIP.	Details shall be shared with successful bidder
2966	43	7.3.3 – UEBA	7.3.3 / 7.3.3.2, Clauses 2–3	UEBA shall continuously monitor users/entities, build behavioural baselines, and configure peer groups, trusted entities and behavioural-analysis parameters.	Please identify the authoritative identity and context sources available for UEBA onboarding (e.g., Active Directory, HRMS, IAM/IGA, PAM, VPN, EDR, DLP, email, physical access), and confirm which source should be treated as the master source for user attributes.	Details shall be discussed with succesfull bidder
2967	43	7.3.3 – UEBA	7.3.3.2, Clause 3	Configured peer groups, trusted entities and relevant behavioural-analysis parameters are required deliverables.	Please confirm the expected peer-grouping dimensions for UEBA (e.g., department, role, designation, branch/location, privileged-user status, employment type) and whether the Bank can provide these attributes from HR/identity systems.	Details shall be discussed with succesfull bidder
2968	43	7.3.3 – UEBA	7.3.3.2, Clause 9	Configured automated response workflows are required for approved high-risk behavioural alerts.	Please identify the UEBA-driven response actions that the Bank expects to automate (e.g., disable account, force password reset, revoke session, isolate endpoint, block IP) and specify which actions require analyst/manager approval.	Details shall be discussed with succesfull bidder
2969	46	7.3.7 – Threat Intelligence Platform	7.3.7.1, Clauses 8–10	The TIP shall support IOC lifecycle management, including creation, validation, enrichment, scoring, distribution, updating and expiration, along with configurable expiry periods and intelligence lifecycle workflows.	Please confirm the expected downstream systems to which curated IOCs/IOAs/TTPs are to be disseminated from the TIP (e.g., SIEM, SOAR, EDR/XDR, firewalls, proxy, email security, NDR), and whether automated push/block actions are expected or only intelligence sharing/enrichment.	Details shall be discussed with succesfull bidder

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2970			Annexure 21 HA table (p.29) read with 7.2.4.1(c) (p.35)	XDR — deployment mode Cloud (SaaS) + Hybrid, with 'Management Console: Deployed at both Primary and Secondary sites'.	For Cloud/SaaS delivered solutions, the Bank is requested to confirm that 'Management Console deployed at both Primary and Secondary sites' means the console is accessible and fully operable from both the DC and the DR site, with platform-side high availability provided in accordance with the Section 13 SLA, RTO and RPO — rather than a customer-hosted console instance physically deployed at each site. Justification: A SaaS console is a single regional console with platform high availability. A physically deployed console at both sites is only possible under a self-hosted model, which the same RFP prohibits for XDR under clause 7.2.4.1(c). The two clauses are mutually exclusive as written.	Please refer addendum for the revised clause
2971			Annexure 21, 16.21.1 and 16.21.2 (p.257-258)	16.21.2 states 'XDR solution for 12,000 users scalable to 14,000'. 16.21.1 separately lists 2,500 servers and 300 databases, alongside 12,000 branch desktops.	The Bank is requested to confirm whether the XDR quantity of 12,000 covers desktops only, or whether the 2,500 servers listed at 16.21.1 are also to be covered within that count. If servers are in scope, the Bank is requested to confirm the split between desktop and server quantities so that both can be quoted correctly. Justification: Section 7.3.4 states XDR coverage 'across endpoints and servers'. If servers are deemed in scope after award, the bid is 2,500 licences short at a different unit price, with no mechanism to re-price. This is the largest commercial exposure on the XDR line.	Please refer addendum for revised clause.
2972			Section 3, clause 6 and clause 11	All Bank data shall reside within India. No Bank data shall be transmitted, replicated, processed, accessed, stored or exchanged outside India without prior written approval from the Bank and applicable regulatory permissions.	The Bank is requested to confirm that OEM technical support and engineering access to Bank data, performed under a documented, logged and auditable process and subject to the Bank's prior written approval as already contemplated in the clause, satisfies this requirement — with all storage and processing remaining within the India region. Justification: Storage and processing within India is achievable. The clause additionally restricts ACCESS, and global OEM support operates on a follow-the-sun basis. Without this clarification the clause cannot be answered 'Complied' truthfully, and Section 15.1 forbids a conditional answer.	No Change, Please be guided by the RFP
2973			Section 7.2.4, Cloud/SaaS table (p.37); Annexure 21, 16.21.3 (p.261)	All Bank-owned data including logs, configurations, policies, rules, reports and metadata shall be backed up / transferred to the Bank's backup infrastructure at DC and DR, with monthly full backups retained in Long-Term Storage for the entire contract duration.	The Bank is requested to confirm whether the endpoint telemetry to be transferred to Bank infrastructure may be scoped to a defined security-relevant subset agreed during implementation and documented in the SOP, rather than the complete raw telemetry stream. Bidders would appreciate an indicative Bank position so that Long-Term Storage can be sized correctly at bid stage. Justification: Unfiltered endpoint telemetry for the proposed estate is of the order of hundreds of GB per day compressed, which over a five-year retention obligation becomes a very large and expensive Bank-side storage requirement. Scoping this at bid stage protects both the Bank's cost and the Bidder's sizing.	No Change, Please be guided by the RFP
2974			Annexure 21, 16.21.2 (p.258-259)	'Each node/environment must be individually provisioned for full peak load' and 'all inline components must operate in high availability mode with automatic failover within seconds'.	For Cloud/SaaS delivered solutions, the Bank is requested to confirm that these requirements apply to the Bank-side components deployed at DC and DR, and that the SaaS platform's availability and capacity are governed by the service levels, RTO and RPO specified in Section 13. Justification: Node-level provisioning commitments cannot be made against multi-tenant SaaS infrastructure. Without this clarification the OEM would be signing an obligation it does not control.	Please refer addendum for the revised clause
2975			Section 3, clause 12	Bank data shall not be used for model training, retraining, analytics, or shared with third parties, whatsoever, except as explicitly authorised by the Bank in writing.	The Bank is requested to confirm whether this restriction is intended to preclude the use of anonymised and aggregated threat indicators for the purpose of improving threat detection efficacy for the Bank's own environment, or whether it is intended to apply without exception. Justification: Determines whether any AI-assisted or threat-intelligence-derived capability can be offered at all, and shapes the OEM's Data Processing Addendum position. Must be settled before the Annexure 18 declaration is signed.	The restriction shall apply without exception unless expressly authorised by the Bank in writing. Bank data, including security telemetry, logs, events, alerts, metadata, threat indicators, and other information generated from or relating to the Bank's environment, shall not be used by the Bidder/OEM for model training, retraining, product improvement, analytics, benchmarking, or any other purpose, nor shared with any third party, unless specifically authorised by the Bank in writing.
2976			Eligibility criteria #24 and #25 (p.210-211); Section 15.1 (p.169)	Minimum 85% functional compliance per solution against Appendix 1A, with exceptions, disclaimers, limitations and conditional compliance not taken on record.	The Bank is requested to confirm whether a response of 'Complied through an additional licensed module included in the commercial offer' is treated as Complied for functional compliance scoring purposes, given that the module concerned is being quoted and supplied as part of the proposal. Justification: Several capabilities are delivered through licensed add-ons that are being priced in the BOQ. Confirming this treatment prevents a technically compliant, fully priced solution being marked down for describing how a capability is licensed.	The compliance of 85% should be met by each of the OEM for their respective Solution & Services as per the eligibility criteria defined.
2977			Eligibility criteria #24 and #25 (p.210-211)	Compliance confirmation and 85% functional compliance are required for each of 14 listed solutions and 9 listed services.	The Bank is requested to confirm that bids comprising multiple OEMs across the listed solutions are permitted, with each OEM providing the Annexure 18 declaration and Appendix 1A compliance for the solutions it supplies. Justification: No single OEM supplies all 14 solutions and 9 services. Confirming the multi-OEM position protects the bid structure.	The compliance of 85% should be met by each of the OEM for their respective Solution & Services as per the eligibility criteria defined.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2978	35, 68-69	Deployment Architecture / On-Cloud	7.2.4 / 7.7	Cloud/SaaS + Hybrid	The RFP specifies Cloud/SaaS deployment for multiple solutions and states that all Bank data, backups, logs, telemetry, prompts and metadata shall reside within India. Please clarify whether the Bank requires all production data, processing, backup, DR, metadata and management/control-plane components to be hosted within India, including the OEM's global cloud control plane.	No Change, Please be guided by the RFP.
2979	69	On-cloud proposed solution OEM Responsibilities	7.7	Data Residency	Please clarify whether OEM technical/support personnel located outside India will be permitted to access Bank data, telemetry, metadata, logs or diagnostic information remotely. If permitted, please specify the approval mechanism and whether such access must be through Bank-controlled privileged access.	Access to such data by OEM personnel located outside India shall not be permitted as part of routine support or operations. In exceptional circumstances, on case to case basis, where offshore access is technically necessary for resolution of a critical incident or specialised support requirement, such access may be permitted only with the Bank's prior written approval and subject to the Bank's applicable security and regulatory requirements. The Bidder/OEM shall disclose in its proposal the location of its support personnel, support centres, data-processing locations and any cross-border data flows or remote-access arrangements relevant to the proposed solution.
2980	69	On-cloud proposed solution OEM Responsibilities	7.7	Data Residency	The RFP states that no Bank data shall be transmitted, processed, stored, validated, replicated or accessed outside India without prior written approval. Please clarify whether temporary diagnostic data, crash dumps, telemetry used for OEM support, threat-intelligence enrichment and anonymized/pseudonymized data are also considered Bank data for this purpose.	Bank data" shall include all information generated from, derived from, relating to, or containing information about the Bank's environment, irrespective of its format, duration, or whether it is in raw, processed, aggregated, anonymized, pseudonymized or encrypted form. The use of anonymization, pseudonymization, aggregation or encryption shall not by itself constitute an exception to the above requirement, without the Bank's prior written approval
2981	69	On-cloud proposed solution OEM Responsibilities	7.7	Data Sovereignty	Please clarify whether the Bank requires the proposed CSP/OEM to provide India-only primary and DR cloud regions, with no cross-region replication outside India.	No Change, Please be guided by the RFP.
2982	69	On-cloud proposed solution OEM Responsibilities	7.7	Data Processing	Please clarify whether processing of security telemetry must also occur within India, or whether only storage/residency is required to be within India.	Any collection, ingestion, processing, correlation, analysis, enrichment, validation, transformation or other handling of such security telemetry shall also take place within India. Any requirement for processing or access outside India shall require the Bank's prior written approval and shall be subject to applicable regulatory, security and contractual requirements.
2983	69	On-cloud proposed solution OEM Responsibilities	7.7	Data Processing	Please clarify whether OEM AI/ML services that process Bank telemetry, alerts, prompts, metadata or threat information must use an India-resident AI/ML processing environment.	Any OEM/Bidder AI/ML capability that processes Bank telemetry, alerts, prompts, logs, metadata, threat information, diagnostic information or any data derived from the Bank's environment shall use an India-resident processing environment.
2984	69	On-cloud proposed solution OEM Responsibilities	7.7	Data Usage	The RFP states that Bank data shall not be used for model training/retraining or analytics except with written authorization. Please clarify whether OEM-native AI/ML features that process telemetry for real-time inference only are permitted without separate approval.	OEM AI/ML capabilities may be used by the Bidder/OEM for providing the contracted services to the Bank
2985	36, 69	Connectivity & Data Privacy	7.2.4.2 / 7.7	Long-term Storage	The RFP requires long-term archival on the Bank's designated archival infrastructure. Please clarify who will provide the archival storage infrastructure, connectivity, backup and archival platform, and whether the bidder is required to include this infrastructure in the BoM.	No Change, Please be guided by the RFP
2986	36	Connectivity and Data Flow	7.2.4.2	Cloud Data Flow	Please provide/confirm the expected data-flow architecture showing which telemetry is required to leave the Bank DC/DR and which data must remain within Bank infrastructure for each Cloud/SaaS solution.	The Bidder/OEM shall provide, as part of its technical proposal, a detailed data-flow architecture for the proposed Cloud/SaaS solution
2987	35	Deployment Architecture	7.2.4	Management Console	The deployment matrix requires management consoles at both Primary and Secondary sites for Cloud/SaaS solutions. Please clarify whether this means actual on-premises management-console components/nodes at DC and DR, or whether secure browser-based access to the SaaS console from both locations is sufficient.	Secure, authenticated browser-based access to the SaaS management console from both DC and DR locations. The SaaS management console meets the availability, uptime & SLA requirements specified in the RFP;
2988	35-36	Deployment Architecture	7.2.4	Cloud/SaaS HA	Please clarify the expected cloud-side HA architecture and minimum availability percentage for each SaaS solution, as the RFP refers to SLA/RTO/RPO but does not provide solution-wise cloud architecture parameters in this section.	The proposed Cloud/SaaS service shall have appropriate redundancy, resilience, fault tolerance and recovery/failover mechanisms to ensure continuity of the contracted services.
2989	35-36	Deployment Architecture	7.2.4	RTO/RPO	Please provide the solution-wise RTO and RPO values applicable to SIEM, SOAR, UEBA, XDR, TIP, CSPM, CNAPP, CWPP and CTEM for the proposed Cloud/SaaS components.	No Change, Please be guided by the RFP
2990	35-36	Deployment Architecture	7.2.4	Cloud DR	Please clarify whether the OEM's native cloud DR mechanism will be accepted for SaaS components, or whether the bidder must provide an independent secondary cloud environment/tenant.	The OEM's to provide the same, such that the proposed DR architecture meets all applicable availability, uptime and SLA requirements specified in the RFP.
2991	36	Connectivity and Data Flow	7.2.4.2	Connectivity	Please clarify whether the Bank will provide Internet/private connectivity, VPN/IPSec, Direct Connectivity, firewall policies and bandwidth required for Cloud/SaaS solutions, or whether these are to be supplied and managed by the bidder.	The hosting space and power arrangements shall be provided by the Bank at the DC and DR locations. The Bank currently has MPLS and Internet services at its DC and DR locations and shall provide the required network connectivity, including MPLS/Internet connectivity, at the Bank's DC and DR locations. Necessary firewall/network changes within the Bank's existing infrastructure shall be coordinated by the Bank and shall be carried out in line with the Bank's policies. Any other components, infrastructure, licenses or services required for the proposed solution shall be factored in by the Bidder within its scope and commercial proposal

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
2992	36	Connectivity and Data Flow	7.2.4.2	Bandwidth	Please provide the expected/available DC-to-Cloud and DR-to-Cloud bandwidth or confirm whether the bidder is required to independently size and provide the required bandwidth.	The Bidder/OEM shall be responsible for assessing and specifying the bandwidth requirement for DC-to-Cloud and DR-to-Cloud connectivity based on the proposed SaaS architecture, expected telemetry/data volumes, peak load, redundancy requirements and performance requirements of the solution. The Bidder shall clearly specify in its technical proposal the minimum and recommended bandwidth required at DC and DR, including peak bandwidth requirements, along with the sizing methodology used.
2993	69	On-cloud proposed solution OEM Responsibilities	7.7	Cloud Landing Zone	The RFP requires a dedicated cloud landing zone with Development, UAT and Production environments. Please clarify whether the Bank already has an approved cloud landing zone/CSP account, or whether the bidder/OEM must provision the complete landing zone from scratch.	The Bidder/OEM shall be responsible for provisioning and configuring the complete cloud landing zone required for the proposed solution. All cloud resources, subscriptions, licenses, configurations, security controls and services required specifically for the proposed solution shall be included in the quoted cost
2994	69	On-cloud proposed solution OEM Responsibilities	7.7	CSP	Please clarify whether the Bank has a pre-approved/mandated CSP, or whether bidders are free to propose the CSP based on compliance with the RFP.	Bidders are free to propose a suitable CSP for the Cloud/SaaS solution, provided that the proposed CSP and architecture fully comply with all requirements of the RFP
2995	69	On-cloud proposed solution OEM Responsibilities	7.7	Cloud Cost	Please clarify whether cloud consumption charges, compute, storage, database, network, API gateway, load balancer, egress/ingress and security-service charges are to be included in the bidder's quoted solution price for the entire contract period.	For Cloud/SaaS solutions, all cloud consumption and service charges required for delivery of the proposed solution shall be included in the Bidder's quoted price for the entire contract period No additional payment shall be made by the Bank on account of increase in cloud consumption, usage, data volume, storage, processing, network traffic or other variable cloud charges during the contract period. All applicable cloud ingress and egress data transfer charges, including charges for data transferred between the Bank's DC/DR environments and the cloud environment, shall be included in the Bidder's quoted solution price for the entire contract period.
2996	69	On-cloud proposed solution OEM Responsibilities	7.7	Cloud Capacity	Please clarify whether the bidder shall absorb cloud consumption growth caused by increased Bank data volumes/users/telemetry during the contract period without additional cost, or whether additional capacity beyond the agreed sizing will be procured separately.	No Change, Please be guided by the RFP
2997	69	On-cloud proposed solution OEM Responsibilities	7.7	BYOK/CMEK	Please clarify whether the Bank will provide its own KMS/HSM for BYOK/CMEK, or whether the bidder/OEM must provide and manage the required KMS/HSM infrastructure.	The Bank is in the process of implementing its KMS infrastructure. Until the Bank's KMS is implemented and made available for integration, the Bidder/OEM shall provide and manage the required KMS/HSM infrastructure and associated licenses/services necessary to support BYOK/CMEK and the proposed solution.
2998	89, 256	IT Infrastructure / Volumetrics	7.18 / Annexure 21	SIEM Sizing	Please confirm the current average EPS, peak EPS, sustained peak EPS and projected annual EPS growth to be used for SIEM sizing.	No Change, Please be guided by the RFP. Refer Annexure 21
2999	256	Sizing/Volumetrics	Annexure 21	SIEM Volume	Please confirm whether the stated SIEM volume represents raw incoming log volume, normalized volume, indexed volume or compressed storage volume for sizing purposes.	No Change, Please be guided by the RFP
3000	256	Sizing/Volumetrics	Annexure 21	SIEM Storage	Please clarify the expected daily TB/day ingestion before and after compression, and the compression ratio that bidders should consider for sizing.	No Change, Please be guided by the RFP
3001	256	Sizing/Volumetrics	Annexure 21	Growth	Please confirm the year-wise growth assumptions for EPS, log volume, users, endpoints, applications, network devices, cloud workloads and security events for the five-year contract period.	Details shall be shared with successful bidder
3002	256	Sizing/Volumetrics	Annexure 21	Retention	Please clarify whether the 60-month retention requirement applies to all SIEM data categories, including raw logs, normalized logs, alerts, incidents, cases, audit trails and forensic data, or only the specified parsed/normalized data.	Please refer addendum for revised clause
3003	256	Sizing/Volumetrics	Annexure 21	Retention	Please clarify whether the one-month raw-log retention and 60-month parsed/normalized retention shall be maintained online/searchable, or whether archival/tiered storage is acceptable after a defined period.	Please refer addendum for revised clause
3004	256	Sizing/Volumetrics	Annexure 21	Archived Data	The RFP requires archived logs and forensic artefacts to be restored in native/readable format. Please clarify the maximum expected retrieval time for archived data and whether archive restoration itself is included within the SLA.	The bidder shall comply with the RTO specified in the RFP. Archive restoration and retrieval required to meet the contractual RTO shall be included in the service scope and shall not attract additional charges
3005	256	Sizing/Volumetrics	Annexure 21	Storage	Please clarify whether archived SIEM data can be stored on Bank-provided storage/object storage, or whether bidder/OEM must provide the complete archive storage infrastructure.	No Change, Please be guided by the RFP
3006	89	IT Infrastructure	7.18	Sizing	Please confirm whether the Bank will provide final server/storage/network/VM specifications, or whether the bidder and OEM are expected to independently derive all physical and virtual sizing from Annexure 21.	No Change, Please be guided by the RFP. Bidder to right size all the required infrastructure.
3007	89	IT Infrastructure	7.18	Growth	Since the bidder bears the risk of incorrect sizing, please clarify the growth percentage or volumetric baseline against which the Bank will determine whether future capacity is due to normal growth or inadequate initial sizing.	Please refer addendum for revised clause
3008	89	IT Infrastructure	7.18	Non-Production	The RFP requires physical separation of production and non-production for on-premise solutions. Please clarify whether a separate physical hardware cluster is mandatory for non-production or whether logically isolated virtualization infrastructure hosted on separate physical hosts is acceptable.	Please refer addendum for revised clause
3009	256	Sizing/Volumetrics	Annexure 21	Non-Production	For VM-based solutions, non-production is stated as minimum 10% of production DC sizing. Please clarify whether this 10% applies to CPU, memory, storage, throughput and licenses independently, or only to compute capacity.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3010	89	IT Infrastructure	7.18	Hardware Age	The RFP requires latest production infrastructure not older than 2025. Please clarify whether this requirement applies to all OEM hardware, storage, switches, appliances and backup equipment, including third-party components embedded within a solution.	Please refer addendum for revised clause.
3011	89	IT Infrastructure	7.18	Staggered Hardware	Please provide the expected implementation/volumetric phases for staggered hardware procurement so that bidders can correctly plan hardware delivery and AMC commencement.	No Change, Please be guided by the RFP
3012	256	Sizing/Volumetrics	Annexure 21	Data Sources	Please provide the indicative number and type of data sources to be onboarded initially and the expected annual growth in data sources for SIEM/XDR/NDR/UEBA.	No Change, Please be guided by the RFP
3013	59	Bidder Responsibilities	7.5	Integration	Please provide the current list of existing SIEM, SOAR, IAM, ITSM, EDR/XDR, network/security, cloud, application and monitoring platforms that must be integrated with the proposed solution.	Details shall be shared with succesful bidder
3014	59	Bidder Responsibilities	7.5	Integration	Please clarify whether integration with future applications/systems introduced by the Bank during the contract period is included without additional cost, and if so, whether there is any limit on the number of such integrations.	Bidder shall support onboarding and integration of all future technologies and log sources during the contract period. All required customizations, enhancements, integrations, and associated workflows, including parsers, connectors, incident workflows, playbooks, and reporting, must be provided without additional cost to the Bank throughout the contract period to the extent they fall within the scope, FRS, TRS, and terms of the RFP or are defined during the SRS stage.
3015	84-86	NextGen SOC Operations	7.15	Custom Parsers/Connectors	The RFP requires custom plug-ins, parsers, connectors, agents and adapters whenever needed without additional cost. Please clarify whether this requirement is unlimited in quantity and applies to all future integrations throughout the contract period.	All required customizations, enhancements, integrations, and associated workflows, including parsers, connectors, incident workflows, playbooks, and reporting, must be provided without additional cost to the Bank throughout the contract period to the extent they fall within the scope, FRS, TRS, and terms of the RFP or are defined during the SRS stage.
3016	59	Bidder Responsibilities	7.5	API/Connector	Please clarify whether any third-party API/connectivity license charges required for integration with existing Bank systems will be provided by the Bank or must be included in bidder pricing.	The bidder shall include all licenses/costs necessary for its proposed solution and required integrations
3017	59	Bidder Responsibilities	7.5	ITSM	Please provide the Bank's existing ITSM platform/version and integration method/API availability for incident/ticket integration with SOC tools.	ITSM - Manage Engine
3018	59	Bidder Responsibilities	7.5	Identity	Please provide the existing IAM/AD/LDAP/SSO/MFA architecture and clarify the required integration scope for all proposed solutions.	Details shall be shared with the successful bidder
3019	36	Connectivity and Data Flow	7.2.4.2	API Integration	Please clarify whether all proposed solutions are required to support bi-directional API/webhook integration, or whether one-way integration is acceptable for specific use cases.	The integration architecture shall depend on the relevant use case. Details shall be shared with the successful bidder.
3020	36	Connectivity and Data Flow	7.2.4.2	Automated Response	Please identify the Bank-approved systems for which automated response actions may be executed by SOAR, such as firewall, EDR, IAM, email gateway, proxy and endpoint controls.	Automated response shall be implemented only on systems/platforms approved by the Bank and in accordance with the Bank's security policies, procedures and change-management requirements.
3021	84	NextGen SOC Operations	7.15	Existing Tools	Please clarify which existing security solutions will be retained, replaced, migrated or decommissioned as part of this project.	Details shall be shared with succesful bidder
3022	95	Transition Management	7.19.2	Existing SIEM	The RFP requires the bidder to run the existing SIEM for 12 months after Go-Live of the respective solutions. Please clarify which existing SIEM platform, deployment architecture, license validity and support arrangement will be available during this period.	Details shall be shared with succesful bidder
3023	29-31	Master Deployment Matrix	7.2.1	N+N Active-Active	Please clarify whether N+N Active-Active means independent N nodes at each DC and DR, with full active processing at both sites, or whether the requirement is limited to N+N redundancy within each site.	Please refer addendum for the revised clause
3024	34-35	Deployment Architecture	7.2.4	HA	Please clarify the expected failover mechanism and failover time between nodes within DC and between DC/DR for each solution.	No Change, Please be guided by the RFP . Refer Section 13 - SLA & Penalty
3025	34-35	Deployment Architecture	7.2.4	HA	Please confirm whether zero/minimal data loss is expected during failure of a DC-side collector/broker/aggregator or whether the applicable RPO permits temporary telemetry loss.	No Change, Please be guided by the RFP . Refer Section 13 - SLA & Penalty
3026	97	DR Setup	7.19.4	DR Readiness	The RFP requires DR setup to be ready on the respective application Go-Live date. Please clarify whether formal DR failover testing must also be completed before Go-Live, or whether readiness and subsequent DR drill are sufficient.	Yes, DR failover testing must also be completed before Go-Live
3027	83-84	DR Drill	7.14	DR Drill	Please confirm the mandatory frequency, expected duration and success criteria for the quarterly NextGen SOC DR drill.	No Change, Please be guided by the RFP, refer section 7.13 Facilities Management
3028	88	System Recovery	7.17	Recovery	Please provide the solution-wise recovery sequence/dependency order expected during a complete DC failure, particularly for SIEM → SOAR → UEBA → XDR → NDR → TIP integrations.	Details shall be shared with succesful bidder during th SRS stage
3029	88	System Recovery	7.17	Recovery	Please clarify whether the bidder is expected to provide a complete end-to-end DR runbook covering Bank infrastructure, network, cloud, OEM and application dependencies, or only the cybersecurity solution layer.	The Bidder/OEM's responsibility for the DR runbook shall be limited to the proposed cybersecurity solution and associated services within the scope of this RFP. The Bidder/OEM shall provide a detailed DR runbook covering the proposed solution components, their dependencies, integrations, configurations, recovery sequence, failover/failback procedures, RTO/RPO and validation steps.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3030	83-88	DR/System Recovery	7.14/7.17	DR Resources	Please clarify whether full L1/L2/L3/OEM manpower is mandatory for every planned and unplanned DR drill and whether the manpower cost is included under FM.	The Bidder/OEM shall provide the required L1/L2/L3/OEM support manpower for all planned and unplanned DR drills, failover/failback activities and associated validation of the proposed cybersecurity solution and services, as required to successfully execute the drill. The manpower and associated support required for such DR drills shall be included in the quoted FM (Facility Management) cost and shall not attract any additional charges to the Bank.
3031	30	Deployment Matrix	7.2.1	NDR	For NDR, please provide the expected network throughput, interfaces, traffic visibility points and packet/flow volume to be used for sizing the NDR appliances.	Details shall be shared with successful bidder
3032	44	NDR	7.3.5	NDR	Please clarify whether the Bank will provide SPAN/TAP/packet-broker connectivity for NDR sensors, or whether the bidder must include required network TAPs/packet brokers in the BoM.	Please refer addendum for the revised clause
3033	44	NDR	7.3.5	NDR Retention	Please clarify the required packet/flow retention period for NDR and whether full packet capture is required or metadata/flow-based monitoring is sufficient.	Please refer addendum for the revised clause
3034	44	XDR	7.3.4	XDR	Please provide the approximate number of endpoints/workloads/users for XDR sizing and confirm expected annual growth.	Please refer addendum for revised clause.
3035	44	XDR	7.3.4	XDR Agents	Please clarify whether XDR agent deployment is expected across servers, workstations, VDI, cloud workloads and containers, and provide the approximate quantity for each category.	Please refer addendum for revised clause.
3036	45	Deception	7.3.6	Deception	Please provide the expected number and location of deception assets/decoys/honeypots and whether the Bank expects coverage across DC, DR, branches, cloud and user networks.	No Change, Please be guided by the RFP
3037	45	Deception	7.3.6	Deception	Please clarify whether the bidder must provide physical/virtual deception infrastructure or whether OEM SaaS-based deception is acceptable wherever technically compliant.	Please refer addendum for revised clause.
3038	42	SOAR	7.3.2	SOAR	Please provide the minimum number of mandatory SOAR playbooks/use cases expected at Go-Live and during O&M.	No Change, Please be guided by the RFP
3039	42	SOAR	7.3.2	SOAR	Please clarify whether custom SOAR playbooks requested by the Bank during the 60-month O&M period must be developed without additional cost and without any limit on quantity.	No Change, Please be guided by the RFP
3040	80	Facilities Management	7.13	AI/ML	The RFP requires data scientists and AI/ML models to reduce L1/L2 activities and false positives without additional cost. Please clarify the expected minimum number of AI/ML use cases/models to be delivered during implementation and O&M.	The bidder shall provide AI/ML capabilities required to achieve the outcomes specified in the RFP at no additional cost to the bank. The number and nature of use cases shall be finalized during implementation based on Bank requirements and the proposed solution.
3041	80	Facilities Management	7.13	AI/ML	Please clarify whether AI/ML functionality may be delivered using the native AI capabilities of the proposed OEM products, or whether the bidder must additionally provide dedicated data-science platforms/resources.	AI/ML capabilities may be used where they demonstrably meet the RFP requirements. The bidder remains responsible for the required outcomes and resources.
3042	80	Facilities Management	7.13	Feature Requests	The RFP requires critical/showstopper feature requests to be implemented within one week. Please clarify whether this applies only to OEM-supported configuration/customization, or also to major product-development features that require OEM engineering changes.	No Change, Please be guided by the RFP
3043	84	NextGen SOC Operations	7.15	Use Cases	Please provide the minimum mandatory detection/use-case catalogue expected for SIEM/UEBA/XDR/NDR and the number of use cases required at Go-Live.	Details shall be discussed with succesfull bidder
3044	84	NextGen SOC Operations	7.15	Detection Engineering	Please clarify whether continuous creation and tuning of detection rules/use cases is included within FM without additional cost, and whether there is any expected monthly/quarterly minimum.	The Bidder/OEM shall provide ongoing tuning based on changes in the threat landscape, threat intelligence, security incidents, false-positive analysis, Bank environment changes and operational requirements. The Bidder shall maintain appropriate documentation and reporting of rules/use cases created, modified, tuned and retired during the contract period.
3045	55	Offsite Services	7.4	Service Scope	Please provide the expected quantity/scope/coverage baseline for each offsite service in Annexure 21, including BAS, CART, ASM, phishing simulation, anti-phishing, dark web, TIP, threat hunting and brand protection.	No Change, Please be guided by the RFP
3046	55	Offsite Services	7.4	Data Access	For offsite services, please clarify whether the service provider will be permitted to receive raw Bank logs/telemetry, or whether only metadata/indicators/anonymized information can be shared.	For offsite services, the Bidder/OEM/service provider shall receive and process only the minimum data necessary to deliver the contracted services. Raw Bank logs, security telemetry or other Bank data may be transmitted to and processed by the service provider only where technically and operationally required for the specific services. Such data shall remain subject to all applicable data residency, security, access-control, confidentiality, retention and data-use requirements specified in the RFP. Where the service can be effectively delivered using metadata, indicators, alerts, threat intelligence, anonymized/pseudonymized or otherwise minimized information, such data shall be preferred over raw Bank data. The Bidder/OEM shall clearly identify, for each offsite service, the type of data collected, whether raw logs/telemetry are required, purpose of processing, processing/storage location, retention period, third-party/subprocessor involvement and data flow. No Bank data shall be used for training, product development or any other purpose beyond providing the contracted services without the Bank's prior written approval.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3047	56-58	Threat Hunting	7.4.8	Remote Access	Please clarify the approved remote-access mechanism through which offsite threat-hunting personnel will access Bank logs, telemetry and security tools.	Through the Bank-approved secure remote-access mechanism and subject to the Bank's security policies and access controls. Access shall be provided on a need-to-know, least-privilege and time-bound basis. Further details shall be shared with the dusccessful bidder
3048	55-58	Offsite Services	7.4	Data Localization	Please clarify whether all platforms used by offsite managed services must also maintain data and processing within India, including dark-web, threat-intelligence, brand-protection and phishing platforms.	All platforms, tools, applications and services used by the Bidder/OEM to deliver offsite managed services shall comply with the Bank's India data-residency and data-processing requirements, including platforms used for dark-web monitoring, threat intelligence, brand protection, phishing simulation/anti-phishing, threat hunting and TIP services. Any Bank data, logs, telemetry, alerts, metadata, credentials, configurations, indicators or other information relating to the Bank shall be hosted, stored, processed, transmitted and accessed only within India.
3049	55-58	Offsite Services	7.4	Takedown	For brand protection/anti-phishing, please clarify whether takedown fees/registrar/platform charges/legal charges are included in bidder scope or will be reimbursed separately by the Bank.	Please refer to the relevant Addendum for updated specfications
3050	55-58	Phishing Simulation	7.4.4	Phishing	Please provide the expected number of employees/users and campaign volume for phishing simulation sizing and pricing.	Please refer 7.2.2 Services for Frequency. The Bidder shall design, in conformity with the bank, the campaign coverage and campaign methodology required to meet the RFP. The proposed service shall support campaigns for the Bank's user base as required by the Bank during the contract period. Campaign design, template creation, reporting and associated activities required to fulfil the RFP shall be included in the Bidder's scope.
3051	57	Dark Web	7.4.6	Dark Web	Please clarify the entities/brands/domains/executives/employee populations that must be monitored under Dark Web Monitoring.	Detailed domain and identity information shall be provided to the selected bidder on a need-to-know basis
3052	57-58	Threat Intelligence	7.4.7/7.4.8	TI/Threat Hunting	Please clarify whether the Bank expects machine-readable threat intelligence feeds/API integration into SIEM/SOAR, or whether portal-based access and reports are sufficient.	No Change, Please be guided by the RFP
3053	47	VA	7.3.8	Vulnerability Assessment	Please provide the approximate number of IP addresses, servers, endpoints, network devices, databases, applications and cloud assets to be covered under VA.	Details shall be shared with successful bidder
3054	48	AST	7.3.10	SAST/DAST	Please provide the approximate number of applications, APIs, repositories and releases per month/quarter to be covered by SAST/DAST.	Details shall be shared with successful bidder
3055	49-53	CSPM/CNAPP/CWPP/CTEM	7.3.11-7.3.14	Cloud Security	Please provide the expected number of cloud accounts/subscriptions/projects, regions, workloads, containers, Kubernetes clusters and cloud assets to be covered.	Details shall be discussed with succesfull bidder
3056	49-53	CSPM/CNAPP/CWPP/CTEM	7.3.11-7.3.14	Cloud Growth	Please provide the expected year-wise growth of cloud accounts, workloads, containers and assets for sizing and licensing.	Details shall be discussed with succesfull bidder
3057	47-53	Security Solutions	7.3.8-7.3.14	Licensing	Please clarify whether licensing for these solutions should be based on the current asset count or the projected five-year maximum volume.	Details shall be discussed with succesfull bidder
3058	47-53	Security Solutions	7.3.8-7.3.14	Additional Assets	Please clarify whether additional assets added by the Bank during the contract period within the quoted volumetric band are included, and how volumes beyond the contracted baseline will be commercially handled.	No Change, Please be guided by the RFP
3059	75	Resource Requirement	7.12.4	L1/L2/L3	Please clarify whether the minimum staffing numbers are per physical location, or whether the listed L1/L2/L3 resources can be distributed across the NextGen SOC office, DC and DR.	The Resource requirement given in the RFP is minimum mandatory requirement that is to be deployed. It includes both DC & DR. Bidder can propose the manpower over and above if required.
3060	75	Resource Requirement	7.12.4	Shift Coverage	Please clarify the shift duration and shift overlap requirement for Shift A, B and C.	Details shall be discussed with succesfull bidder
3061	75	Resource Requirement	7.12.4	Backup Manpower	Please clarify the expected minimum backup/reliever ratio to maintain 24×7×365 availability during leave, training, absence and attrition.	The bidder shall ensure adequate backup/reliever resources to maintain uninterrupted 24×7×365 service availability during leave, training, absence, attrition, or any other unplanned/unavoidable circumstances. The bidder shall deploy sufficient qualified resources, complying at least the minimal requirement, to ensure that the required service levels and contractual obligations are not impacted at any time.
3062	75	Resource Requirement	7.12.4	OEM SME	Please clarify the expected minimum OEM SME availability/response time for each of the 14 solutions during critical incidents.	The bidder shall ensure that adequate OEM support arrangements, including backup resources, are maintained throughout the contract period
3063	75	Resource Requirement	7.12.5	Additional Resources	The RFP requires additional resources at no additional cost whenever required. Please clarify whether this applies to temporary incident surge resources only or permanent additional manpower throughout the contract period.	The bidder shall deploy additional resources at no additional cost where required to meet its contractual obligations, SLAs, implementation requirements, incident surges, leave/reliever requirements or performance obligations.
3064	73-75	Resource Requirement	7.12	Named Resources	Please clarify whether Bank approval is required for every L1/L2 resource replacement, or only Key Resources.	No Change, Please be guided by the RFP
3065	73-75	Resource Requirement	7.12	OEM Resources	Please clarify whether OEM SME personnel are required to be onsite in India, or whether remote OEM SME support is acceptable except where onsite presence is specifically requested.	The bidder shall ensure that adequate OEM support arrangements are in place to meet the required service levels throughout the contract period. The Bank will not provide remote access to its systems/network/environment to the bidder or OEM SME personnel.
3066	95	Transition Management	7.19.2	Existing SOC	Please provide the complete inventory of existing SOC solutions, OEMs, versions, architecture, licenses, support contracts and current implementation status to enable transition planning.	Details shall be shared with succesful bidder

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3067	95	Transition Management	7.19.2	Existing SIEM	Please provide the current SIEM's EPS, TB/day, retention, number of sources, architecture and current license entitlement for the 12-month post-Go-Live support period.	Details shall be shared with succesful bidder
3068	95	Transition Management	7.19.2	Incumbent	Please clarify the expected knowledge-transfer period and formal handover process from the incumbent service provider to the selected bidder.	Please refer addendum for the exit management clause. Further details will be shared with successful bidder
3069	95	Transition Management	7.19.2	As-Is Support	During the “as-is and where-is” support period, please clarify whether any existing-system performance/security issues caused by the incumbent architecture will remain the Bank's responsibility or become the selected bidder's responsibility.	The bidder shall conduct an initial assessment and document known defects/dependencies during transition. the bidder remains responsible for operating, securing and supporting the transitioned environment to meet SLAs.
3070	95	Transition Management	7.19.2	Existing Licenses	Please clarify who will bear the cost of existing SIEM/solution license renewals required during the transition and 12-month coexistence period.	The existing SIEM shall continue to be operated for a period of 12 months after Go-Live of the proposed SIEM, primarily to support regulatory, audit and transition requirements. The Bidder shall be required to provide necessary support for the continued running of the existing SIEM during this period on best effort basis.
3071	95	Transition Management	7.19.2	Coexistence	Please clarify whether the existing SIEM and new SIEM will need to operate simultaneously with duplicate log ingestion, and whether the additional infrastructure/storage required for coexistence is included in bidder scope.	The existing SIEM shall continue to be operated for a period of 12 months after Go-Live of the proposed SIEM, primarily to support regulatory, audit and transition requirements. The Bidder shall be required to provide necessary support for the continued running of the existing SIEM during this period on best effort basis.
3072	99	Project Timelines	Section 9	5-Month Implementation	Please clarify whether the five-month implementation period begins from PO acceptance/T0, irrespective of Bank dependencies such as site readiness, connectivity, access, data availability and incumbent handover.	No Change, Please be guided by the RFP
3073	99	Project Timelines	Section 9	Dependencies	Please clarify whether delays caused by Bank-provided infrastructure, network connectivity, access approvals, third-party vendors, incumbent service provider or Bank UAT sign-off will result in corresponding timeline relief.	No Change, Please be guided by the RFP
3074	99	Project Timelines	Section 9	Go-Live	Please clarify whether all 14 solutions and 9 managed services must achieve full Go-Live within the same five-month period, or whether solution-wise phased Go-Live is permitted.	Solution Wise phase go-live is permitted. However the timeline of 5 Month period remains sacrosanct
3075	64	Deployment & Go-Live	7.6.5	UAT	Please provide the expected UAT acceptance criteria, UAT duration and sign-off authority for each solution.	No Change, Please be guided by the RFP
3076	64	Deployment & Go-Live	7.6.5	VAPT/IS Audit	Please clarify whether VAPT/IS Audit will be conducted by the Bank's appointed agency or by the bidder/OEM, and whether remediation must be completed before UAT or before Go-Live.	VAPT/IS Audit shall be conducted by the Bank or its appointed/authorized agency, as applicable. The bidder/OEM shall provide all necessary support, information, documentation, and cooperation required for conducting such assessments. The detailed VAPT/IS Audit requirements, Go-Live checklist, and preparedness criteria shall be discussed and finalized with the successful bidder during the implementation phase.
3077	64	Performance Testing	7.6.5	Performance Testing	Please provide the mandatory performance test benchmarks for response time, throughput, CPU, memory, storage, failover and recovery for each solution.	No Change, Please be guided by the RFP
3078	64	Hypercare	7.6.5	Hypercare	Please clarify the required duration of the post-Go-Live hypercare period and the minimum onsite/OEM resources required during hypercare.	No Change, Please be guided by the RFP
3079	63-64	Documentation	7.6.4/7.6.5	Documentation	Please provide the mandatory document acceptance checklist for HLD, LLD, SCD, SOP, as-built, DR, test, UAT and Go-Live documentation.	No Change, Please be guided by the RFP
3080	80	Facilities Management	7.13	Patching	Please clarify the expected SLA/TAT for applying critical, high, medium and low-risk OEM security patches after release.	No Change, Please be guided by the RFP
3081	80	Facilities Management	7.13	Vulnerability Remediation	Please provide the exact critical/high/medium/low vulnerability remediation timelines applicable to the proposed solutions.	No Change, Please be guided by the RFP
3082	69	On-cloud	7.7	Cloud Patch	Please clarify whether the bidder/OEM is responsible for patching the underlying CSP-managed infrastructure, or only the application/platform components under bidder control.	The bidder/OEM shall be responsible for ensuring compliance with all applicable security, patching, hardening, and regulatory requirements for the proposed solution and all components proposed as a part of the overall solution/services
3083	98	Contract Period	Section 8	EOL/EOS	Please clarify whether the requirement to replace EOL/EOS components at no additional cost applies to SaaS products and cloud services, including changes in OEM subscription editions/SKUs.	No Change, Please be guided by the RFP
3084	95	Other Scope Activity	7.19	Feature Changes	The RFP states that committed features must remain available even if the OEM changes its licensing model. Please clarify whether the bidder must provide equivalent functionality without additional cost even where the OEM discontinues the original product edition.	No Change, Please be guided by the RFP
3085	35 of 122	XDR	4.13	The goal is to minimize the attack surface by continuously monitoring, updating, and provide compensatory controls for vulnerabilities and exploits in the endpoints	We request to modify this clause as below "The goal is to minimize the attack surface by continuously monitoring, updating, and provide visibility for vulnerabilities and exploits in the endpoints" Justification: The term "visibility" is outcome-focused and technology-agnostic, allowing solutions to detect and report vulnerabilities through various mechanisms (signatures, behavioral analysis, real-time scanning, etc.), whereas "compensatory controls" is overly prescriptive and implies specific mitigation techniques that may not be applicable to all vulnerability types or endpoint environments. Changing to "visibility" maintains the security intent while enabling bidders to propose diverse, fit-for-purpose solutions without unnecessary implementation constraints.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3086	35 of 122		12	The proposed solution must provide protection against malicious AI application tampering on the endpoints	We request to modify this clause as below "The proposed solution must provide protection against malicious applications tampering on the endpoints" Justification:The "AI" qualifier is overly specific and may exclude non-AI malware threats, creating coverage gaps. The broader term "malicious application tampering" aligns with industry-standard endpoint protection language and ensures comprehensive threat protection regardless of the attack vector or technology employed.	No Change, Please be guided by the RFP
3087	36 of 122		15	The proposed XDR solution must provide comprehensive activity data management and search capabilities, including receiving activity data in the form of telemetry, and metadata; feature for automatic query runs and email notifications; threat matching features using Boolean Logic and other criteria; and options to export, import, delete, and share saved search queries.	We request to modify this clause as below: The proposed XDR solution must provide comprehensive activity data management and search capabilities, including receiving activity data in the form of telemetry, and metadata; feature for automatic query runs and email notifications; threat matching features using Boolean Logic and other criteria; and options to export, delete, and share saved search queries. Justification:The "import" functionality is not a core operational requirement for XDR activity data management. The primary requirements are exporting queries for backup/sharing, deleting obsolete queries, and sharing queries among team members—all of which are standard XDR capabilities. Import functionality introduces unnecessary complexity, potential security/governance risks from external query sources, and is not universally supported across commercial XDR solutions, thereby limiting vendor options unnecessarily	No Change, Please be guided by the RFP
3088	36 of 122		22	The solution should offer options to leverage anti-malware and anti-spyware components stored locally on agents, or signatures stored in-the-vendor cloud	From the operational context and use cases for each deployment option, ensuring continuity of threat protection in all connectivity scenarios. By explicitly defining "when offline" (local components) and "when online" (cloud signatures), the clause removes ambiguity regarding the solution's capability to maintain protective coverage during network disconnections while leveraging updated threat intelligence when connectivity is available We request to modify this clause as below "The solution should offer options to leverage anti-malware and anti-spyware components stored locally on agents when offline, or signatures stored in-the-vendor cloud when online."	No Change, Please be guided by the RFP
3089	36 of 122		29	The solution Device Control capability must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The solution Device Control capability must support Network Devices, USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, time based device control capabilities allowing admin to define the policy specifically for the endpoint operating systems (Windows 10, 11 or higher).	We request to modify the clause as below: The solution Device Control capability must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The solution Device Control capability must support USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, allowing admin to define the policy specifically for the endpoint operating systems (Windows 10, 11 or higher)to allow the devices as required. Justification: Network Devices are typically managed through enterprise network security controls and firewalls rather than endpoint Device Control, and time-based controls create unnecessary operational complexity and maintenance overhead. The modified clause focuses on high-risk local device vectors (USB, Mobile Storage, Bluetooth, Modems) that pose direct security threats to endpoints, while allowing flexibility for organizations to enable specific devices based on business requirements.	No Change, Please be guided by the RFP
3090	37 of 122		43	The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature or through seamless integration with a third-party sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data	We request to amend this clause as below: The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data. Justification: To ensure operational independence and reduce implementation complexity, the organization requires native sandbox functionality built into the core solution rather than relying on third-party integrations, which introduce external dependencies, potential single points of failure, and increase support overhead. This modification mandates that bidders deliver complete sandboxing capability as an integrated component from day 1, ensuring seamless functionality, consistent vendor accountability, and simplified maintenance and support operations without external vendor coordination.	Please refer addendum for revised Clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3091	38 of 122		57	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	We request to amend this clause as below: The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture or 99.9% availability SLA distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead. Justification: The modification provides architectural flexibility while maintaining the Bank's core availability objective. Not all qualified SaaS vendors employ Active-Active multi-AZ architecture; however, industry-standard 99.9% SLA meets enterprise-grade requirements and enables broader vendor participation without compromising operational resilience. This alternative approach is vendor-agnostic, measurable, and backed by contractual guarantees rather than architectural prescriptions.	Please refer Addendum for revised clause
3092	37 of 122		42	The proposed solution should provide recommended actions to address and mitigate threats detected on endpoints. These remediation suggestions should be informed by forensic data collected from endpoints and detailed analysis performed by the solution to enhance threat response and resolution.	To ensure accurate cost proposals and licensing calculations, please clarify the estimated forensics data volume requirements: a) What is the expected monthly forensics data volume (in GB) that the solution must support? b) What is the planned retention period for forensics data? c) Does this volume include forensics data from all sources (endpoints, servers, cloud workloads, network) or specific sources only? This clarification will enable all bidders to calculate appropriate licensing models and provide consistent cost estimates	Details shall be shared with the successful bidder
3093	54 of 122	Cloud Security	4	The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud envirionment like AWS/Azure/GCP/Meghdoot, AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.	We request to modify this clause as below The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud envirionment like AWS/Azure/GCP/ AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports. Justification: Meghdoot is a comprehensive open-source cloud suite, but bringing it up to PSB requirements demands significant development and integration effort. To be effective, the target cloud environment must be seamless, eliminating the overhead of custom modifications.	Please refer addenudm for revised clause The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud envirionment like AWS/Azure/GCP, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.
3094	Addition of Point as recommendatio n	Cloud Security	To be Added in Cloud Security	The proposed solution should also support the File scanning with no limitation on file/object type or size covering application across organisation. This should include but is not limited to Amazon Simple Storage Service (S3), Amazon FSx amd Amanzon Elastic File System.	Benefit to PSB: Comprehensive file scanning eliminates critical security blind spots across the organization's cloud storage infrastructure, ensuring no malware, ransomware, or sensitive data can be inadvertently stored in S3, FSx, or EFS without detection. By removing file type and size limitations, the solution prevents attackers from bypassing scanning through obfuscation or leveraging uncommon formats, while the multi-storage coverage consolidates security posture across diverse AWS storage services under a single unified policy. This provides unified threat visibility, enables regulatory compliance (HIPAA, PCI-DSS, GDPR), prevents data exfiltration, and protects against insider threats and supply chain compromises affecting cloud-stored data—significantly reducing the risk of ransomware attacks, compliance violations, and unauthorized data exposure.	No Change, Please be guided by the RFP
3095	page 30 of 273	Extended Detection & Response (XDR)	5	Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Cloud (SaaS): HA Deployment aligned with the SLA, RTO & RPO (Refer Section 13). Management Console: Deployed at both Primary and Secondary sites	We request to amend this clause as below: Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Cloud (SaaS): HA Deployment aligned with the SLA, RTO & RPO (Refer Section 13). Justification: In Appendix 1A clause 27 under XDR explicitly mention for SaaS "ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead" Though it's a SaaS based the management console cannot be deployed at both primary and secondary sites.	Please refer addendum for revised clause
3096	page 31 of 273	Cloud Workload Protection Platform (CWPP)	13	Cloud (SaaS): Deployment aligned with the SLA, RTO & RPO (Refer Section 13).. Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Management Console: Deployed at both Primary and Secondary sites	We request to amend this clause as below: Cloud (SaaS): Deployment aligned with the SLA, RTO & RPO (Refer Section 13).. Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Justification: For SaaS solution the management console cannot be deployed at banks primary & secondary site	Please refer addendum for revised clause
3097	Page 38 of 122 & Page 38 of 122	XDR	22 to 35	These points are duplicate need to be removed	These points are duplicate need to be removed	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3098	29, 35 & 259	Sections 7.2.1, 7.2.4.1(b) & 16.21.2	Section 7.2.1	Deception deployment and high-availability topology (Deception Technology): "Any agent/Enforcer/Deceptor Standalone at DC and HA, N+N, Standalone at DR." Section 7.2.4.1(b): "The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active configuration." Section 16.21.2 (Decoy): "All the inline components of the solution must operate in high availability mode. In the event of any component failure, the system should automatically initiate failovers within seconds, ensuring uninterrupted functionality without requiring manual intervention."	The RFP describes the Bank-side deception components as standalone in Section 7.2.1, point no.- 4, but it is also mentioned HA and N+N. We request the bank to kindly clarify that in case we're deploying the solution on-prem, whether Bank needs the solution in Standalone mode/HA mode/N+N mode. Section 16.21.2 (Decoy), point no.-8, Bank has asked that all the inline components of solution should be in HA mode with automatic failover capability. However, the deception solution is not inline. Hence, we request Bank to clarify if they need the Deception Solution in HA. We request the Bank to add on-prem solution also in addition to Cloud/SAAS+Hybrid.	Please refer addendum for revised clause
3099	45, 261 & 262	Sections 7.3.6.2(2) & 16.21.3 - Deployment and Data Retention	Section 7.3.6.2(2):	Backup, restoration and log-retention requirements "Restore the logs/data from backup for forensic investigation and as per bank requirement without any additional cost." Section 16.21.3: "Duration of the Contract (Monthly Full backup) - Long-Term Storage (LTS) - Entire Duration of the Contract." The RFP further states that applicable Monthly Full Backups shall be migrated to LTS at the Bank's DC & DR and retained for the entire duration of the contract.	We request bank to kindly confirm that if the bank will provide the storage for backup.	No Change, Please be guided by the RFP. Bidder to right size and provide all the required infrastrcuture as per RFP
3100	68	Section 7.7 - On-cloud proposed solution OEM Responsibilities, Point 10	"The OEM shall have valid ISO/IEC 27001 certification and SOC 2 Type II report."	Cloud OEM certification requirement	We request the bank to accept ISO/IEC 27001 or SOC 2 Type II or both.	No Change, Please be guided by the RFP
3101	29, 32 & 35	Sections 7.2.1, 7.2.3 and 7.2.4.1(b)	Section 7.2.1 (Deception Technology): "Cloud (SaaS) + Hybrid" Section 7.2.3: "The solution shall be hosted through a Cloud Service Provider (CSP), either fully as a SaaS service or through a combination of CSP-hosted and Bank-hosted components." Section 7.2.4.1(b): "Deception Technology: The core Deception platform shall be deployed in the	Responsibility for providing the Cloud/SaaS environment	7.2.4.1(b) We request the bank to kindly add the on-prem implementation option also for the core component of the Deception Solution.	Please refer addendum for revised clause
3102	35 & 91	Sections 7.2.4.1(b) and 7.18.1 - Compute Infrastructure, Point 1	Section 7.2.4.1(b): "Deception Technology: The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active configuration. The Cloud/SaaS deployment shall be aligned with the applicable SLA, RTO and RPO requirements."	Hardware and VM infrastructure for Bank-hosted deception components	We request the bank to kindly add the on-prem implementation option also for the core component of the Deception Solution.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3103	84	Breach and Attack Simulation (BAS)	Sl. No. 1 - Technical Specification	The solution should simulate Ransomware Attacks	Rationale for change: The clause as drafted is a single unqualified statement that every bidder in this category will mark compliant, so it cannot differentiate responses against the 10 marks allotted. It also does not define what constitutes a ransomware simulation. A ransomware validation exercise is only meaningful to the Bank if the platform reproduces the tradecraft ransomware operators actually use, including vulnerable driver loading to terminate endpoint protection, and does so without causing damage on production assets. The Bank is requested to replace the clause with testable criteria covering safe execution of destructive behaviours, deterministic cleanup, and kernel-level attack testing. Proposed modified clause: The proposed solution must execute structurally authentic attacks with destructive elements neutralised, and must be able to trigger destructive-technique detections without the harmful action (for example, testing volume shadow copy deletion detection without deleting the volume shadow copy). It must provide deterministic cleanup mechanisms, safe for execution on production assets, including backup, restore, and removal of all artifacts across: a. File b. Registry c. Service	No Change, Please be guided by the RFP
3104	84	Breach and Attack Simulation (BAS)	Sl. No. 3 - Technical Specification	The ability to simulate infiltration techniques for breaching a network or infecting a host	Rationale for change: "Infiltration techniques" is undefined and cannot be evaluated objectively. Initial access is the stage at which the Bank's email gateway, secure web gateway and web application firewall are tested, and current adversary tradecraft delivers initial access through container formats such as ISO, IMG, MSI, LNK and ZIP, followed by execution that avoids system interpreters in order to bypass AMSI, script block logging and constrained language mode. A clause that names these delivery and execution requirements allows the Bank to compare bidders on demonstrable capability rather than on a general claim. Proposed modified clause: The proposed solution must dynamically generate container-format payloads including ISO, IMG, MSI, LNK, and ZIP variants containing executables, shortcuts, or DLL hijack chains, and deliver them via uniquely generated URLs per simulation to comprehensively validate email gateway, secure web gateway, and WAF filtering against modern initial-access techniques such as ISO-LNK-DLL chains. The simulation agent must execute malicious behaviours and adversary techniques without reliance on system interpreters including PowerShell, CMD, BASH, or SH, validating control effectiveness against modern adversary tradecraft that increasingly avoids interpreter-based execution to bypass AMSI,	No Change, Please be guided by the RFP
3105	84	Breach and Attack Simulation (BAS)	Sl. No. 6 - Technical Specification	The solutions should test Security Operations Center (SOC) detection capability of bank by simulating multi-chained payloads with advanced evasion methods including DLL Hijacking, Process Injection, and PPID spoofing for breaching and infiltrating the network.	Rationale for change: The clause names only three evasion techniques and does not state that they must be executed as real behaviours on the asset rather than logged as simulated steps. SOC detection validation succeeds or fails on two things the clause does not capture: whether the payload natively performs modern evasion against the deployed control stack, and whether each technique is available in multiple procedure variants, since a detection that catches one implementation of LSASS credential dumping routinely misses six others. The Bank is requested to expand the clause so that detection coverage is validated across the attacker variant space. Proposed modified clause: The simulation payload execution must natively perform the following techniques as executed behaviours against the deployed control stack: a. EDR unhooking (NTDLL unhooking, direct and indirect syscalls) b. Reflective DLL injection c. Process hollowing d. PPID spoofing e. Command-line argument spoofing f. Fileless in-memory execution For each in-scope MITRE ATT&CK technique, the proposed	No Change, Please be guided by the RFP
3106	84	Breach and Attack Simulation (BAS)	Sl. No. 7 - Technical Specification	The solution should have the ability to create custom use cases / simulations attacks according to bank's requirement.	Rationale for change: As drafted the clause is satisfied by a script upload field or by a vendor professional services engagement, both of which leave the Bank dependent on the OEM for every new scenario and carry recurring cost. For the Bank's own security team to build scenarios for proprietary applications and internal workflows, the clause should require a user interface driven attack creator with named configurable parameters. Proposed modified clause: The proposed solution must provide a UI-driven attack creator enabling customer security teams to design custom multi-stage simulations with configurable name, description, MITRE category, execution privileges (User/Admin), payload type (DLL/EXE/Service/ISO/MSI/LNK), and chained secondary behaviours supporting organisation-specific scenario testing for proprietary applications, internal workflows, and bespoke attack hypotheses.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3107	84	Breach and Attack Simulation (BAS)	Sl. No. 8 - Technical Specification	The solution must allow the execution of simulations on multiple agents simulataneously. An attack chain must be executed on multiple endpoints agents at the same time to provide unique attack specific insights across the deployed agents in the organisation.	Rationale for change: The clause states the requirement for simultaneous execution but does not exclude sequential execution presented as a single campaign, which is how several solutions in this category operate. It also does not address the operational prerequisites for running simulations across a bank-scale estate: the agent must be deployable at scale through Group Policy or golden image, must run silently so that branch and business users are not alerted or disrupted, and must update centrally without re-imaging or desk visits. The Bank is requested to make both the concurrency model and the deployment model explicit. Proposed modified clause: The proposed solution must execute a single coordinated attack campaign across multiple agents, business units, and geographies simultaneously, not sequentially (i.e. One Kill chain, run on multiple Endpoint Targets at the same time), producing independent per-agent evidence consolidated into a unified campaign report. Solutions that walk through agents one-by-one cannot realistically validate enterprise-scale concurrent compromise scenarios. The simulation agent must be a lightweight software package suitable for enterprise mass-deployment via Group Policy Object (GPO), golden image baking, or standard endpoint management tooling, requiring no per-host configuration post-installation.	No Change, Please be guided by the RFP
3108	84	Breach and Attack Simulation (BAS)	Sl. No. 11 - Technical Specification	The solution should support technical integrations with bank's existing solutions (e.g., SIEMs, ticketing systems, log management, Firewalls, automation/orchestration, analytics solutions, threat intelligence solutions, etc.)	Rationale for change: "Should support technical integrations" is unverifiable and is routinely answered with roadmap commitments or bespoke development quoted after award. For closed-loop validation, where a simulation result is correlated against the alert raised in the Bank's SIEM and a ticket is created automatically, the Bank needs a documented API, automation tooling and pre-built connectors available at the time of bid. The Bank is requested to make the integration requirement specific and verifiable. Proposed modified clause: The proposed solution must expose a RESTful API with publicly available OpenAPI documentation, provide an open-source CLI and SDK for automation, and ship pre-built integrations with major SIEM, SOAR, ITSM, EDR, firewall, and email gateway vendors to enable closed-loop validation of alerts, automated ticket creation, and detection correlation.	No Change, Please be guided by the RFP
3109	30	RFP - 7.2 Solution & Services Deployment Model and Their HA Requirement 7.2.1 Solutions – Master Deployment Matrix	6. Network Detection & Response (NDR)	Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Management Console: Deployed at both DC and DR	Different NDR solution works on different redundancy deployment methodology (I.e Active - Active or Active - Passive). Request bank to modify the clause as: Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active/Passive at DC and HA, N+N, Active-Active/Passive at DR. Management Console: Deployed at both DC and DR	Please refer addendum for revised clause
3110	45	RFP - Scope of Work 7.3.5 Network detection and response (NDR)	7.3.5.1 Modules, Architecture & Deployment:	Pt 2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Generally NDR solutions are deployed with sole purpose of doing network analysis, threat detection & response and does not have native 2FA capability, so request bank to remove this point. As an alternate as proposed in same point, proposed NDR solution can be integrated with bank's existing MFA solution.	Please refer addendum for the revised clause
3111	49	RFP - Scope of Work 7.3.10 Application security testing Tool	7.3.10.1 Modules, Architecture & Deployment:	Pt 2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Generally AST solutions are deployed with sole purpose of scanning the source code, web, api etc and does not have native 2FA capability, so request bank to remove this point. As an alternate as proposed in same point, proposed AST solution can be integrated with bank's existing MFA solution.	No Change, Please be guided by the RFP
3112	110	RFP - 10.2 Eligibility Evaluation Criteria	OEM Evaluation Criteria	Pt 19. The proposed OEM SIEM Solution with a minimum capacity of 30,000 EPS or 1.2 TB/day shall have been successfully implemented on cloud in one (1) in India.	For wider participation, we request bank to amend the clause as: The proposed OEM SIEM Solution with a minimum capacity of 5,000 EPS or.2 TB/day shall have been successfully implemented on cloud in any one (1) Govt/PSU customer in India. OR The proposed OEM SIEM Solution with a minimum capacity of 10,000 EPS or.4 TB/day shall have been successfully implemented on cloud in one (1) in India.	Please refer addendum for revised clause.
3113	112	RFP - 10.2 Eligibility Evaluation Criteria	OEM Evaluation Criteria	Pt 20. The proposed OEM solution should have been implemented in at least one BFSI is to be submitted for the following solutions: NDR	For wider participation, we request bank to amend the clause as: The proposed OEM solution should have been implemented in at least one BFSI / Govt is to be submitted for the following solutions: NDR	Please refer addendum for the revised clause
3114	260	RFP - 16.21.2 Volumetrics- Solution-wise Requirements	12. Application Security Testing Tool	All the inline components of the solution must operate in high availability mode. In the event of any component failure, the system should automatically initiate failovers within seconds, ensuring uninterrupted functionality without requiring manual intervention.	Application Security Testing as a technology in general works at developemnt/pre-production/UAT stage only. And hence as a solution there is no need of high availability mode. Same has already been updated in this RFP (as solution is asked in standalone at both DC & DR). So, request bank to deleted this clause.	No Change, Please be guided by the RFP. The bidder must design the solution to fully comply with the RFP requirements, ensuring that in case of a failover, the system meets the defined SLA for availability, RTO, and RPO. The bidder is required to adhere to the deployment requirements outlined in the RFP when designing and proposing the solution architecture.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3115	40	APPENDIX 1A Functional Compliance Sheet (Solutions)	Network Detection & Response (NDR)	Pt 8. Proposed solution should generate a root cause analysis, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets.It should provide a platform for easier investigation like visual graphical view and timeline of the attack and it should support tagging of MITRE tactics, techniques and procedures used by the attacker in alerts and incidents.	We reqeust bank to amend the clause: Proposed solution should generate a root cause analysis / incident management, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets.It should provide a platform for easier investigation like visual graphical view and timeline of the attack and it should support tagging of MITRE tactics, techniques and procedures used by the attacker in alerts and incidents.	Please refer addendum for the revised clause
3116	40	APPENDIX 1A Functional Compliance Sheet (Solutions)	Network Detection & Response (NDR)	Pt 13. The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	As bank has asked for on-premise solution for NDR, on the contrary, this clause asks for cloud-native SAAS ask. So, we kindly request bank to delete this clause.	Please refer Addendum for revised clause
3117	42	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 3. The solution must be able to analyse a wide array of programming languages including Java,.Net, C/C++, Objective-C, Android, PHP, COBOL, Ruby, Swift, HTML 5, Scala, APEX, TypeScript, Go, Kotlin and ABAP etc but not limited to these alone	Considering the future requirements of AI in Secure Code Development and most of the development is moving towards AI generated code using AI supported languages. So it is very important for bank to have coverage around this as well and will recommend to incorporate AI supported languages like "R, Ada, Solidity, Bash, Groovy, Rust, Perl", but not limited to these alone.	No Change, Please be guided by the RFP
3118	42	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 24. Solution should support Machine learning and Analysis based on the archived results	ML capability is important, but it is very important to have coverage around AI based code as well. And will recommend bank to consider: The solution should have the capability to scan AI generated code. The solution should be able to integrate with AI coding agent via MCP	No Change, Please be guided by the RFP
3119	43	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 32. The solution should be able to support Composition Analysis: Identify the opens source components used in the application. Vulnerabilities & outdated version Licensing risk associated with the components	Bank is looking for Software composition analysis and asked for identifying the open source component and licensing risk. But this limited information is not enough for bank to secure themselves with rapidly increasing supply chain attacks and we will highly recommend to consider following as well: SCA system must catalogue open source components from Maven, NPM, and Nuget. SCA system has to be able to generate a Bill of Materials for an application. Solution should have the ability to continuously monitor the scanned components & notify if there are any zero day attacks without performing the rescan. Solution should Catalog, Store, and Audit SBOMs (both cycloneDx & SPDX) generated for in-house developed software applications and COTS applications.	No Change, Please be guided by the RFP
3120	30	7.2 Solution & Services Deployment Model and Their HA Requirement 7.2.1 Solutions – Master Deployment Matrix	Sl. No. 8	Vulnerability assessment (VA) & vulnerability lifecycle management Bank Location: Standalone at DC and Standalone at DR. Management Console: Deployed at both DC and DR	Requesting clarifications if standalone management console in DR will be live or will be on standby ?	Please refer addendum for revised clause
3121	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 1 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall be deployable entirely on-premises and shall not require any cloud-hosted component, external service, or Internet connectivity for its core functionality, scanning, management, reporting, analytics, or product capabilities.	Requesting change to: The proposed solution shall be deployable entirely on-premises or hosted on MeitY cloud or Meity empanelled cloud environment. No data shall be shared with the platform/cloud outside India geolocation.	Please refer addendum for the revised clause
3122	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 3 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall be software-based and fully deployable on the hardware infrastructure proposed by the Bidder.	Requesting change to: The proposed solution shall be software-based and fully deployable on the hardware infrastructure or should support hybrid- on-premise architecture with management-console or scanners on on-premise and analytics components on MeitY/MeitY-emapanneled cloud proposed by the Bidder.	No Change, Please be guided by the RFP
3123	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 9 of Vulnerability Assessment & vulnerability lifecycle Management	Each scanning engine shall support web application security assessment together with traditional infrastructure vulnerability and configuration/compliance assessment. The solution shall identify vulnerabilities, missing patches, insecure configurations, and compliance deviations, and generate comprehensive reports containing risk severity, evidence of findings, affected assets, and remediation recommendations to support security governance, audit, and regulatory compliance.	Requesting to confirm that if DAST specs are specifically provided for web-application's VAPT, then what is the scope of "web-application" scanning in this spec? Also requesting to share the total number of web-applications considered in the scanning scope.	No Change, Please be guided by the RFP
3124	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 18 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall support both active and passive asset discovery and vulnerability assessment/scanning.	Requesting change to: The proposed solution shall support both active and/or passive asset discovery and vulnerability assessment/scanning.	No Change, Please be guided by the RFP
3125	48	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 27 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall support both active and passive techniques for vulnerability detection, where applicable.	Requesting change to: The proposed solution shall support both active and/or passive techniques for vulnerability detection, where applicable.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3126	48	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 33 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall support deployment and lifecycle management of scanning agents without dependency on cloud-hosted services.	Requesting change to: The proposed solution shall support deployment and lifecycle management of scanning agents.	No Change, Please be guided by the RFP
3127	48	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 34 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall assess Active Directory security posture and identify misconfigurations, privilege risks, insecure policies, and exposure of critical directory services.	Requesting to clarify that this spec is already addressed in IDTR then what is the requirement of it in VM solutin?	No Change, Please be guided by the RFP
3128	49	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 74 of Vulnerability Assessment & vulnerability lifecycle Management	The solution shall support offline signature and plugin updates for deployment in isolated or air-gapped environments.	Requesitng to remove this spec because if the cloud-based solution is offered and where cloud is hosted on MeitY cloud or MeitY empanneled cloud then questions related to air-gap environment doesn't arise.	No Change, Please be guided by the RFP
3129	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 81 of Vulnerability Assessment & vulnerability lifecycle Management	The solution shall support password-protected and/or digitally signed reports with configurable retention and archival.	Requesting change to: The solution must support secure, encrypted report distribution (including native PGP encryption) and enforce strict role-based access controls (RBAC) for report viewing. Additionally, the platform must provide configurable cloud-based data retention policies alongside automated options to archive historical scan data and reports to external storage	No Change, Please be guided by the RFP
3130	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 87 of Vulnerability Assessment & vulnerability lifecycle Management	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	Requesting change to: The solution must provide AI-generated risk summaries and plain-language vulnerability briefs that automatically fuse asset criticality, technical findings, and real-world threat telemetry (such as CISA KEV and EPSS data) to streamline IT triage. If cloud analytics are utilized to run these machine learning models, the solution vendor must guarantee that all data is isolated within dedicated, bank-authorized cloud regions, employing strict data privacy frameworks that ensure source code, credentials, and raw scan parameters are explicitly excluded from public AI training models or multi-tenant public AI services	Please refer addendum for revised clause
3131	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 88 of Vulnerability Assessment & vulnerability lifecycle Management	Unified, correlated findings intelligence. Every scanning engine — across web, API, network and host, cloud, containers, mobile, source code, device configuration and identity — reports into a single normalized findings model..	Requesting clarification on why unified reporting is asked as the ASM, VM, DAST solutions are considered separately.	No Change, Please be guided by the RFP
3132	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 90 of Vulnerability Assessment & vulnerability lifecycle Management	Mobile Application Security Testing: The proposed solution shall support static security analysis of Android and iOS mobile application packages, including APK/AAB and IPA formats, and shall provide security assessment mapped to recognized mobile application security standards and methodologies such as OWASP MASVS and MASTG.	Requesting clarification for the spec as the ask is for DAST or MAST solution.	No Change, Please be guided by the RFP
3133	87	Anti Phishing Services	17.1	Solution should detect at the earliest point in the attack, post initial compromise as the attacker is first attempting to move laterally and escalate privilege.	Since this section is focused on Anti-Phishing, we understand that the objective is to identify suspicious activity following a successful phishing or account-compromise event. Network-level lateral movement and deception capabilities may be addressed by other security controls. We request the Bank to clarify whether this clause may instead focus on early post-compromise user activity visibility for the Bank's most critical users. " The solution should support early identification and investigation of suspicious user activities associated with potential account compromise following phishing or other email-originated attacks, with enhanced user activity monitoring for up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles."	Please refer to the relevant Addendum for updated specfications
3134	87	Anti Phishing Services	17.4	Solution must provide robust supply chain and AI/ML-driven contact chain analysis capabilities to identify and defend against socially engineered, impersonated, or BEC attacks.	As compromise of trusted suppliers and partners is an important source of BEC and phishing risk, we request the Bank to clarify whether the existing supply-chain requirement should explicitly include behavioural analysis of supplier/partner communication patterns to identify attacks originating from compromised trusted accounts. " Solution must provide robust supply-chain and AI/ML-driven contact-chain and behavioural analysis capabilities to identify and defend against socially engineered, impersonated or BEC attacks, including threats originating from compromised or impersonated supplier/partner accounts."	Please refer to the relevant Addendum for updated specfications
3135	87	Anti Phishing Services	18	Solution must proactively analyze suspicious URLs using dynamic/behavioral analysis to prevent the spread of malware and other threats.	The RFP separately addresses URL analysis and post-delivery remediation. We request clarification whether these requirements are intended to provide continuous protection throughout the email threat lifecycle, including pre-delivery analysis, click-time URL protection and post-delivery detection/remediation. " Solution must provide continuous protection across the email threat lifecycle, including pre-delivery threat detection, real-time/click-time inspection of suspicious URLs, and post-delivery detection and automated remediation of threats that are subsequently determined to be malicious."	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3136	88	Anti Phishing Services	19.7	Solution must be able to offer a comprehensive portal that allows users to access information and metadata on events/incidents, facilitating network threat forensics for thorough investigation and analysis of potential security breaches or incidents.	To strengthen investigation of phishing-led incidents involving executives and other critical users, we request clarification whether the existing forensic portal requirement may also include contextual user and endpoint activity for a limited population of Bank-identified critical/high-risk users. " Solution must offer a comprehensive investigation portal providing information and metadata on events/incidents for forensic analysis. For up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, the portal should additionally provide contextual user and endpoint activity, including relevant application, file and user-action details, to support investigation of potential phishing-led compromise."	Please refer to the relevant Addendum for updated specfications
3137	88	Anti Phishing Services	19.9	Solution must empower security operations and incident responders to automate the identification, remediation, and sharing of phishing threats, streamlining the process of detecting, addressing, and disseminating information about potential phishing attacks for improved response and mitigation.	To improve SOC investigation efficiency, we request clarification whether the existing phishing identification and remediation requirement should include centralized attack context showing why a message was identified as malicious, the users targeted, associated threat indicators and remediation status. " Solution must empower security operations and incident responders to automate identification, investigation, remediation and sharing of phishing threats, and should provide centralized contextual visibility into the users targeted, associated threat indicators, detection rationale, attack characteristics and remediation actions."	Please refer to the relevant Addendum for updated specfications
3138	88	Anti Phishing Services	19.1	Solution must provide incident responders with real-time analytics and visibility into email-based attacks targeting the organization.	Email-based attacks against executives and privileged users may require additional context after delivery to determine whether a targeted user has subsequently performed suspicious activity. We request the Bank to clarify whether real-time investigation visibility may include relevant user activity context for up to 100 Bank-identified critical/high-risk users. " Solution must provide incident responders with real-time analytics and visibility into email-based attacks targeting the organization. For up to 100 Bank-identified critical/high-risk users, the solution should additionally provide contextual visibility into suspicious user activities associated with potential phishing or account compromise, including relevant user, endpoint, application and file activity."	Please refer to the relevant Addendum for updated specfications
3139	88	Anti Phishing Services	19.23	Solution must have simplicity of evaluation and additional visibility into internal traffic and other communication channels can reduce risk, and baseline user activity to detect suspicious behavior.	The existing clause already seeks baselining of user activity to detect suspicious behaviour. We request the Bank to clarify the intended depth and scope of this capability and whether enhanced monitoring may be applied to a focused population of up to 100 Bank-identified critical/high-risk users, where deeper visibility provides the greatest security value. " Solution must provide additional visibility into relevant internal activity and communication channels to reduce risk and baseline user activity to detect suspicious behaviour. Enhanced user and data activity monitoring should be provided for up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, with configurable detection policies for suspicious, anomalous or policy-violating activities."	Please refer to the relevant Addendum for updated specfications
3140	90	Anti Phishing Services	19.7	Solution must provide protection against harassment mail and mitigate the risks associated with emails from unknown senders specifically for executives or VIPs, safeguarding them from potential threats and ensuring their email communication remains secure.	Since this clause already provides enhanced protection for executives/VIPs, we request the Bank to clarify whether such enhanced protection should extend beyond receipt of suspicious email to investigation of risky user and data activities that may occur following phishing or account compromise, for a limited set of the Bank's most critical users. "Solution must provide protection against harassment mail and mitigate risks associated with emails from unknown senders specifically for executives or VIPs. For up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, the solution should additionally provide enhanced visibility into risky user and data activities following suspected phishing or account compromise, including relevant file movement, web/upload activity, removable-media activity and other supported data-transfer channels."	Please refer to the relevant Addendum for updated specfications
3141	52	Idendity Threat Detection and Response (ITDR)	1.7	Detect and respond to active threats with high fidelity (low false positives and false negatives).	The Bank has separately specified a comprehensive deception platform for detection of active attacker activity, reconnaissance and lateral movement. We understand that the intent of this clause within ITDR is therefore to complement those controls with focused monitoring of the Bank's most critical identities. Considering that enhanced user-activity monitoring is most relevant for high-risk personnel such as executives, privileged users and other critical users, we request the Bank to kindly clarify whether this requirement may be read as follows: " Identity Threat Detection Solution should provide high-fidelity detection and response for risky or anomalous user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, to identify activities associated with careless, malicious or compromised users. "	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3142	52	Idendity Threat Detection and Response (ITDR)	1.8	Provide contextual information—who, what, when and how—to inform all stages of the attack chain.	The Bank has already sought attack-lifecycle visibility under the separate deception requirements. For ITDR, we understand that additional value would be derived from detailed user-centric context for the Bank's most critical identities, enabling investigation of risky activity performed by such users. We request the Bank to kindly clarify whether this requirement may be read as follows: " Identity Threat Detection Solution should provide contextual information—who, what, when, where and how—around risky user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, to support investigation and response."	No Change, Please be guided by the RFP
3143	52	Idendity Threat Detection and Response (ITDR)	1.9	Provide deep insights into both the potential and used privilege escalation and lateral movement steps in an attack.	Privilege escalation and lateral-movement visibility is already substantially addressed under the separately specified deception solution, including attacker lifecycle visibility, MITRE ATT&CK mapping, deceptive attack paths and detection of lateral movement. To avoid duplication while retaining complementary investigation capability for high-risk identities, we request the Bank to kindly clarify whether this requirement may be read as follows: "Identity Threat Detection Solution should provide deep insights into activities performed by up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, covering application usage, file and data movement, endpoint activity and other risky behaviours to support investigation of compromised, malicious or negligent user activity."	No Change, Please be guided by the RFP
3144	52	Idendity Threat Detection and Response (ITDR)	2.9	Detect all types of attack vectors including pre-attack reconnaissance, zero-day attacks, privilege escalation prevention, lateral movement and data theft.	Pre-attack reconnaissance, lateral movement, malware/attack behaviour and attacker lifecycle visibility are already covered under the Bank's separate deception specifications. We understand that the complementary requirement under ITDR should focus on identity/user risk and potential data-loss activity for the Bank's most critical users rather than duplicate the deception control. We request the Bank to kindly clarify whether this requirement may be read as follows: " Identity Threat Detection Solution should detect risky user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, including suspicious application usage, unauthorized access or movement of sensitive information, removable-media activity, web-based transfer, cloud synchronization and other potential data-exfiltration activities."	The Clause is applicable only to idendity related threat vector only. The volumetrics is provided in the RFP and should be complied
3145	52	Idendity Threat Detection and Response (ITDR)	2.10	Detect multiple attacks simultaneously.	We understand the intent is to ensure that the solution is not restricted to investigation of a single event at a time. Since active attacker detection is separately covered by the deception solution, we request that this clause be clarified in terms of concurrent monitoring and investigation of risky activities across the Bank's designated critical-user population: "Identity Threat Detection Solution should be capable of detecting and investigating multiple risky user and data activities simultaneously across up to 100 critical/high-risk users and their monitored endpoints."	No Change, Please be guided by the RFP
3146	52	Idendity Threat Detection and Response (ITDR)	3.2	Provide unified presentation of both source- and target-based telemetry data in a timeline view.	The Bank has separately specified end-to-end attacker visibility and behavioural analysis under the deception solution. For ITDR investigations involving critical identities, a chronological user-activity view would provide complementary evidence of actions performed by the user. We request the Bank to kindly clarify whether the requirement may be read as follows: " Identity Threat Detection Solution should provide a unified chronological timeline of user- and endpoint-based activity telemetry for up to 100 critical/high-risk users identified by the Bank to support investigation of risky or suspicious user activity."	No Change, Please be guided by the RFP
3147	52	Idendity Threat Detection and Response (ITDR)	3.3	Correlate identity-related telemetry from relevant source and target systems to identify and investigate identity compromise, privilege escalation, credential abuse and lateral movement.	Privilege escalation and lateral-movement detection are already addressed through the separately specified deception controls. To provide complementary investigation capability for the Bank's highest-risk identities, we request the Bank to clarify whether this clause may focus on correlation of user, endpoint, application and data activity for the designated critical-user population: " The solution shall support correlation of user, endpoint, application and data-activity telemetry for up to 100 critical/high-risk users identified by the Bank to identify and investigate suspicious user behaviour, sensitive-data movement, policy violations and potential data-exfiltration activities."	No Change, Please be guided by the RFP
3148	52	Idendity Threat Detection and Response (ITDR)	3.4	Integrate with compatible endpoint/extended detection solution to capture screen recordings or screenshots during active attacker sessions as advanced forensic evidence.	The Bank has separately specified attacker-session and forensic visibility through the deception platform. Within ITDR, we understand that visual evidence is intended to strengthen investigation of high-risk user activity. We request the Bank to kindly clarify whether the requirement may be read in an outcome-based manner for the designated critical-user population: " The Identity Threat Detection Solution should support screenshots, screen capture or equivalent visual evidence of relevant activity for up to 100 critical/high-risk users during suspicious or high-risk user sessions, as part of forensic investigation and evidence collection."	Please refer addendum for revised clause.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3149	52	Idendity Threat Detection and Response (ITDR)	3.5	Integrate with compatible network detection solution to support collection of PCAP data for network-level incident visibility.	The requirement for PCAP is network-centric and does not directly relate to identity posture or focused user-activity monitoring. Further, the Bank's separate deception specifications already require high-interaction decoys, recording of attacker activities, traffic/behaviour visibility, forensic investigation and integration with network/security technologies. To avoid duplication of network-level forensic controls across two solution categories, we request the Bank to kindly delete this clause from the ITDR section.	Please refer addendum for revised clause.
3150	52	Idendity Threat Detection and Response (ITDR)	3.6	Push incident data into SIEM/XDR or SOAR technologies via integrations for improved incident management.	We understand that the objective is to ensure relevant ITDR alerts and investigation context are available to the Bank's SOC ecosystem. For the enhanced monitoring of designated critical users, we request the Bank to kindly clarify whether alerts and activity information may be shared through supported integrations or APIs as follows: " Identity Threat Detection Solution should make alerts and relevant incident/activity data for the monitored critical-user population available to SIEM/XDR, SOAR or other supported security platforms through integrations or APIs for improved incident management."	The proposed solution hould be integrated with SIEM/XDR or SOAR technologies for sharing the incident data via supported integrattion or APIs
3151	52	Idendity Threat Detection and Response (ITDR)	3.7	As part of forensic data collection, include detailed attack path information including protocols leveraged during the attack.	Detailed attack-path and attacker-behaviour visibility is already sought under the separate deception specifications, including deceptive attack paths, MITRE ATT&CK mapping and forensic investigation. To avoid overlap while retaining complementary evidence for investigations involving the Bank's critical identities, we request the Bank to kindly clarify whether the requirement may be read as follows: " Identity Threat Detection Solution should, as part of forensic data collection for up to 100 critical/high-risk users, include detailed user-activity information such as applications used, files accessed, data movement, destination channels and other relevant endpoint activity associated with the incident."	Please refer addendum for revised clause
3152	52	Idendity Threat Detection and Response (ITDR)	3.8	Collect user and computer information from Active Directory as part of forensic data gathering to enhance context and assess risk exposure.	We understand that directory information is required to enrich investigations with user and computer context. We request the Bank to clarify that enterprise identity context may be maintained for the overall identity population, while detailed endpoint/user-activity telemetry may be applied to the Bank's designated critical-user population: " Identity Threat Detection Solution should use relevant user and computer identity information to enhance forensic context and risk assessment, and should correlate such context with detailed endpoint/user-activity telemetry for up to 100 critical/high-risk users identified by the Bank."	Please refer addendum for revised clause
3153	52	Idendity Threat Detection and Response (ITDR)	3.9	Detect an adversary's attempt to move laterally toward key assets using as many Windows, Mac or Linux hosts as possible without requiring a persistent agent.	The Bank's separate deception specifications expressly require detection of lateral movement, reconnaissance, credential theft and malicious activity using agentless and/or agent-based deception techniques across the enterprise. The present clause therefore duplicates a capability already being procured under the Deception section. To avoid overlapping scope and duplicate controls, we request the Bank to kindly delete this clause from the ITDR section.	Please refer addendum for revised clause
3154	52	Idendity Threat Detection and Response (ITDR)	3.10	Collect AD user/computer information for forensic context and detect at the earliest point post initial compromise as the attacker first attempts lateral movement and privilege escalation.	Early detection of lateral movement and privilege-escalation activity is substantially covered under the Bank's separate deception requirements. To retain a complementary identity/user-risk objective without duplicating the deception scope, we request the Bank to kindly clarify whether this clause may focus on early detection of risky activity among the designated critical-user population: " Identity Threat Detection Solution should use relevant identity context and detect risky user behaviour at the earliest possible point for up to 100 critical/high-risk users, based on monitored endpoint activities and configured detection policies, enabling investigation and response before such activity results in significant data loss or business impact."	Please refer addendum for revised clause
3155	52	Idendity Threat Detection and Response (ITDR)	3.11	Collect AD user/computer data during forensic gathering while ensuring all deception techniques remain hidden from legitimate users.	The requirement to ensure deception techniques remain hidden from legitimate users is inherently a deception-platform capability. The Bank has already included comprehensive deception requirements covering lures, breadcrumbs, fake credentials, deceptive assets, attacker engagement and techniques designed to remain undetected by attackers. We therefore request the Bank to kindly delete this clause from the ITDR section to avoid duplication.	Please refer addendum for revised clause.
3156	2	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	10	OEM shall ensure compliance of the complete proposed solution & platform with RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and all applicable regulations throughout the contract period.	We request the Bank to clarify that the OEM is required to maintain applicable security, privacy and regulatory controls relevant to the services provided and furnish available compliance/assurance documentation, while the overall regulatory compliance obligation of the Bank remains subject to the Bank's deployment, configuration and usage of the service. " OEM shall maintain security, privacy and compliance controls applicable to the proposed hosted service and shall provide available independent assurance reports, certifications and relevant compliance documentation to support the Bank's obligations under applicable RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and other applicable regulatory requirements."	Please refer addendum for revised clause
3157	2	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	20	The Service uptime agreement for the proposed solution on cloud should have monthly uptime commitments and have transparent monthly credit calculations in case of uptime not being met for any services.	We understand that published/contracted OEM hosted-service SLA commitments and corresponding service-credit methodology shall meet this requirement. Kindly confirm.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3158	3	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	29	Solution provider should provide the design and process for data deletion in the scope of an independent audit and that the operational effectiveness of these controls is tested. The report for the same should be submitted to bank as and when asked by bank.	For a globally operated hosted security service, control effectiveness is generally evidenced through independent assurance reports such as SOC 2 Type II and documented data-retention/deletion controls. We request the Bank to permit such independent assurance documentation instead of requiring a separate bespoke data-deletion audit report. " Solution provider shall maintain documented secure data-retention and deletion controls. Compliance may be demonstrated through applicable independent third-party assurance reports/certifications (such as SOC 2 Type II or equivalent) and documented data-retention/deletion policies made available subject to OEM confidentiality requirements."	Please refer addendum for the revised clause
3159	4	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	41.3	Independent audit for testing effectiveness of secure data removal, such that data is rendered permanently inaccessible. (Including any backup or distributed online media).	We request the Bank to accept independently audited secure deletion and media-management controls, together with documented retention/deletion periods, rather than requiring a customer-specific audit of all backup and distributed media. " The OEM shall maintain secure data deletion, media handling and backup-retention controls designed to render customer data inaccessible in accordance with documented retention schedules. Effectiveness may be evidenced through independent assurance reports such as SOC 2 Type II/ISO 27001 or equivalent and relevant OEM security/privacy documentation."	Please refer addendum for the revised clause
3160	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	47.2	Bank shall have an option to implement 'Bring Your Own Key' as and when required.	The proposed service protects data at rest and in transit using strong encryption; however, customer-managed infrastructure encryption keys are not a standard capability of the hosted anti phishing service. We request deletion of the BYOK requirement, or acceptance of OEM-managed enterprise-grade encryption and key-management controls. " Requested Action: Delete the BYOK requirement. Alternatively: 'Data processed/stored by the hosted service shall be protected using industry-standard encryption in transit and at rest, with secure OEM-managed key-management controls subject to independent security assurance.'"	Please refer addendum for the revised clause
3161	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	49	Web Application Firewall shall be implemented on the cloud for Web based applications. WAF application signature should be updated and reviewed regularly. The Report shall be submitted to bank on a periodic interval.	Since the proposed platform is an OEM-managed hosted security service, underlying WAF technology, signatures and configurations form part of the OEM's internal security architecture and may not be exposed as customer-specific reports. We request the Bank to accept periodic VAPT/penetration-test assurance or equivalent independent security assessment evidence covering the hosted application instead of WAF signature reports. " The hosted web application/platform shall be protected through appropriate application-security controls. The OEM shall conduct periodic vulnerability assessment and penetration testing/security assessments and, subject to confidentiality restrictions, provide an executive summary/attestation or applicable independent assurance evidence to the Bank on request. Customer-specific WAF signature reports shall not be mandatory."	Please refer addendum for revised clause
3162	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	52	The systems in cloud infrastructure should be periodically updated with the latest anti-malware signatures, the bidder shall submit the periodic report on the same with bank.	For an OEM-managed hosted security service, infrastructure anti-malware/endpoint controls are centrally managed and independently audited. We request the Bank to accept OEM security assurance and vulnerability/malware-control attestations rather than periodic host-level signature reports. " The OEM shall maintain appropriate malware protection, vulnerability management, patching and security monitoring controls for the hosted infrastructure. Compliance may be evidenced through independent assurance reports/certifications and applicable security-control attestations instead of customer-specific anti-malware signature update reports."	Please refer addendum for revised clause
3163	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	53	Data Loss Governance and risk management framework shall be defined by bidder for workload on the cloud and same shall be shared with bank on periodic basis. Data loss prevention controls should be implemented to secure the data in the cloud environment from unauthorized or inadvertent exfiltration.	We request clarification that the requirement is intended to ensure protection against unauthorized/inadvertent data exfiltration through the proposed service and appropriate security controls for hosted customer data, rather than requiring disclosure of the OEM's internal cloud governance framework. " The proposed solution shall provide configurable controls to identify and prevent unauthorized or inadvertent transmission/exfiltration of sensitive information through any channels. The OEM shall maintain appropriate access control, encryption and data-protection controls for customer data processed within the hosted service and provide applicable assurance documentation on request."	Please refer addendum for revised clause
3164	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	81	Log generation, storage and review process should be certified by CERT IN empaneled auditor, report for the same shall be submitted by bidder as and when required by bank.	For global SaaS/POD services, security logging and monitoring controls are typically independently audited under recognized assurance frameworks. We request the Bank to accept SOC 2 Type II/ISO 27001 or equivalent independent assurance in lieu of a mandatory CERT-In-empanelled audit of the OEM's internal log-generation/storage/review process. " The OEM shall maintain documented security logging, monitoring, retention and review controls. Effectiveness shall be evidenced through applicable independent third-party assurance reports/certifications such as SOC 2 Type II, ISO 27001 or equivalent. CERT-In-empanelled audit may be required only for bidder-managed components deployed specifically within the Bank environment, where applicable."	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3165	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	82.5	IT Act 2000 & its amendments, and other Acts/Regulatory guidelines.	Kindly clarify that the OEM must comply with legal/regulatory requirements applicable to it as the provider of the proposed hosted service and provide reasonable documentation to support the Bank's compliance obligations. " OEM shall comply with applicable legal and regulatory obligations relevant to its provision of the proposed service and shall provide available security/privacy/compliance documentation reasonably required to support the Bank's applicable obligations."	Please refer addendum for the revised clause
3166	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	83	CERT IN Empaneled auditor report's is required for the following:	We request the Bank to permit internationally recognized independent assurance reports/certifications for OEM-managed hosted services. CERT-In empanelled audit reports may remain applicable to India-specific bidder-managed/on-premises components where such audit is feasible and required. " For OEM-managed hosted/SaaS services, independent assurance reports/certifications such as SOC 2 Type II, ISO 27001 or equivalent shall be accepted. CERT-In empanelled audit reports shall be applicable only to components/services for which such India-specific audit is contractually and technically feasible."	Please refer addendum for the revised clause
3167	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	92	The application and DB is/will be hosted separately on a dedicated infrastructure (physical/logical) for PSB. Evidence of dedicated infrastructure (physical/logical) for PSB should be submitted.	The proposed platform is an OEM-managed hosted security service designed with logical access controls and customer data isolation. Requiring dedicated physical application/database infrastructure would restrict standard SaaS/POD architectures without necessarily improving the security outcome. We request acceptance of secure logical tenant/customer isolation supported by independent assurance evidence. " The proposed hosted service shall provide secure logical segregation/isolation of Bank data and administrative access from other customers through appropriate access-control and tenant-isolation mechanisms. Dedicated physical application/database infrastructure shall not be mandatory where equivalent logical isolation is implemented and independently assured."	Please refer addendum for the revised clause
3168	8	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	98.1	Feasibility to audit/review IT controls of the third party or obtaining independent review report for the same from CERT-In empaneled security consultant, to ensure it meets Bank's information security requirement.	We request that the Bank permit review of current independent assurance reports/certifications as the primary mechanism for reviewing OEM IT controls. Any direct audit should remain subject to the OEM's standard contractual audit provisions, confidentiality, security, scope and advance-notice requirements." The Bank may review applicable independent third-party assurance reports/certifications covering the hosted service. Where additional audit is required, such audit shall be subject to mutually agreed scope, confidentiality/security restrictions, reasonable advance notice and the OEM's standard contractual audit provisions. A CERT-In empanelled consultant may review evidence made available under these conditions."	Please refer addendum for the revised clause
3169	Appendix 1A Page 40	NDR Functional Compliance Sheet	Clause 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high- availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	The Clause mandates Cloud based SaaS model, while RFP Page 30, Page 35, section 7.2.4.1 clause 'd' asks for on Premesis solution "The NDR shall be deployed On-Premises". We request to modify the clause to include On-Prem solution. Justification: To include solutions which are on-Prem based	Please refer Addendum for revised clause
3170	Appendix 1A Page 40	NDR Functional Compliance Sheet	Clause 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high- availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	The Clause asks for Active-Active HA architecture, we request to include Active-Standby Mode. Justification: Management Console is central console, it cannot be deployed in Active-Active mode, as it is a central component.	Please refer Addendum for revised clause
3171	Appendix 1A Page 41	NDR Functional Compliance Sheet	Clause 18	Solution should have the capabilities to create and run security playbooks for automation and better MTTD/MTTR on the basis of criticality of threat/server	Proposed solution adopts below appraoch for automated MTTD, Solution need investigative workflows and all the alerts need to be validated before building any Active Response Solution is having inbuilt playbooks like Host, Session and Packet analysis. once alert is validated Active Response can be triggered. Hope the approach is acceptable	Please refer addendum for the revised clause
3172	Page 66	7.6.7	Training	At a minimum, the following training programs shall be conducted for each proposed solution / OEM appointed officials: Duration per Session and Munimum Number of Sessions	Overall there is a requirement of 15 Sessions and Duration per session is 2 or 3 days. This takes the total training per solution to 40 days. This is very large reqirement of training, we request to make it to 3 days for NDR solution	Please refer addendum for revised clause
3173	Page 63	7.6.6	Testing, clause 3	The bidder shall provision and maintain dedicated Development, Testing, UAT, and Pre-Production environments throughout the contract period.	Is UAT Environment required for NDR solution also, given that NDR is a Passive and out of path solution.	Please refer addendum for revised clause
3174	30, 34	7.2.1 Deployment Model & HA (TIP) / 7.2.4.1 Deployment Pattern	Table 7.2.1 Sr. 7; Cl. 7.2.4.1(e)	"Threat Intelligence Platform (TIP) - Cloud (SaaS) + Hybrid - Bank Location: Broker/Collector/Integrator: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR" (Table 7.2.1).	Cyble's Threat Intelligence Platform (TIP) is delivered as a fully cloud-native SaaS solution, providing continuous threat-intelligence aggregation, enrichment and distribution to the Bank via API, STIX/TAXII feed and a dedicated web portal, with high availability, geographic resiliency and disaster recovery built into the SaaS platform itself - fully aligned with the SLA, RTO and RPO defined in Section 13. As the TIP's core function requires no packet-level or in-line processing within the Bank's network, Cyble can meet the Bank's continuity requirement for this solution without deploying a broker/collector component on Bank premises. We request the Bank's confirmation that this cloud-native delivery model will be accepted as fully compliant with Table 7.2.1.	Please refer addendum for the revised deployment requirement

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3175	31, 35	7.2.1 Deployment Model & HA (CSPM) / 7.2.4.1 Deployment Pattern	Table 7.2.1 Sr. 11; Cl. 7.2.4.1(i)	"Cloud Security Posture Management (CSPM) - Cloud (SaaS) + Hybrid - Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR" (Table 7.2.1); "...with the required connectors, collectors, agents, enforcers and/or other supporting Bank-side components, if required, deployed at the Bank's DC and DR in N+N Active-Active configuration" (Cl. 7.2.4.1(i)).	Cyble's Cloud Security Posture Management (CSPM) module continuously assesses the Bank's cloud environments through secure, read-only, API-based/cross-account IAM-role integration, with no agent, connector or collector required on Bank premises. This lets Cyble deliver continuous, real-time cloud security posture monitoring with high availability and resilience built natively into the SaaS platform, fully meeting the Bank's SLA, RTO and RPO requirements under Section 13. This is consistent with the qualifying language "if required" already present in Cl. 7.2.4.1(i). We request the Bank's confirmation that this API-integrated, cloud-native delivery model will be accepted as compliant.	Please refer addendum for the revised clause
3176	55-56	7.4.3 Attack Surface Management	Cl. 7.4.3	"Discovery of internet-facing and internal assets... The proposed solution shall provide AI-enabled Attack Surface Management (ASM) capabilities for continuous discovery... of the organization's external attack surface, including known and unknown internet-facing assets."	Cyble's Attack Surface Management (ASM) capability provides continuous, AI-enabled discovery, monitoring and risk-prioritization of the Bank's entire external attack surface - internet-facing assets, exposed services, domains, cloud assets and shadow IT - using external/passive reconnaissance together with Bank-shared asset inventories (IP ranges, domains, cloud accounts), with no agent or appliance required inside the Bank's network, consistent with the offsite Managed Service model in Section 7.2.2. This gives the Bank a complete outside-in exposure view from Day 1. We request the Bank's confirmation that this externally-led, agentless approach satisfies Cl. 7.4.3.	Bank is looking for external attack surface management
3177	55	7.4.5 Anti-Phishing	Cl. 7.4.5	"...offsite continuous anti-phishing monitoring and response services for detection, analysis for phishing attacks targeting the Bank, its employees, customers, executives, digital assets, domains, and online channels."	Cyble is fully equipped to deliver continuous, 24x7 Anti-Phishing monitoring across the Bank's domains, executives and digital channels from Day 1 of the engagement, scaling seamlessly as the Bank's digital footprint grows, with no additional infrastructure required from the Bank. To finalise the onboarding plan, we request the Bank share the number of primary/registered domains, sub-domains, executive/VIP identities and customer-facing digital channels to be covered at contract commencement, so Cyble can confirm precise sizing against this scope.	Please refer to the relevant Addendum for updated specfications
3178	57	7.4.6 Dark Web Monitoring	Cl. 7.4.6	"...offsite, tool-based continuous dark web and cyber threat exposure monitoring services... across the surface web, deep web, dark web, underground forums, messaging platforms, and data leak repositories."	Cyble's Dark Web & Cybercrime Monitoring capability continuously covers the surface web, deep web, dark web, underground forums, messaging platforms and data-leak repositories, and can begin protecting the Bank's specified identities, brand keywords and domains immediately upon contract signature. To tailor this coverage precisely, we request the Bank share the initial monitoring scope (employee/executive identities, brand keywords, domains and relevant data categories) so Cyble can confirm sizing and reporting cadence.	Details shall be shared with succesful bidder
3179	57	7.4.7 Threat Intelligence Feed	Cl. 7.4.7(l)	"Provision of threat intelligence through a centralized portal/dashboard and/or machine-readable feeds."	Cyble's Threat Intelligence Feed is delivered through both a centralized portal/dashboard and machine-readable, standards-based feeds (STIX/TAXII, MISP-compatible formats and API), enabling seamless integration with the Bank's existing or future security stack whenever required. We confirm this dual delivery model - portal-based consumption plus machine-readable feed/API - and request the Bank's confirmation that it satisfies Cl. 7.4.7.	No Change, Please be guided by the RFP
3180	57-58	7.4.8 Threat Hunting Services	Cl. 7.4.8(m)	"The threat hunting service shall be delivered remotely/offsite using secure and mutually agreed mechanisms for accessing relevant logs, telemetry, security tools, and data made available by the Bank."	Cyble can deliver proactive, intelligence-driven Threat Hunting entirely offsite - correlating curated external threat intelligence (IOCs, IOAs, TTPs, threat-actor and campaign intelligence) against Bank-shared context, supplemented by secure, mutually agreed read-only access to relevant Bank telemetry for validation and deeper investigation as needed - fully consistent with the remote/offsite delivery model mandated in Cl. 7.4.8(m). We request the Bank's confirmation that this intelligence-led hunting model, combined with agreed read-only telemetry access, meets the Bank's requirement.	No Change, Please be guided by the RFP
3181	58	7.4.9 Brand Protection and Monitoring	Cl. 7.4.9(j)	"Takedown coordination with relevant registrars, hosting providers, platforms, application stores, social media platforms, and other relevant entities, wherever applicable."	Cyble's Brand Reputation Monitoring capability continuously identifies brand impersonation, typosquatting, phishing/fraudulent websites, fraudulent mobile apps and social-media impersonation, and actively coordinates takedown requests with registrars, hosting providers, app stores and social platforms on the Bank's behalf under a standard authorisation executed at contract signature - delivering a fully managed, end-to-end takedown process with minimal effort required from the Bank's team. We request the Bank's confirmation that this bidder-led takedown coordination model satisfies Cl. 7.4.9(j).	Please refer addendum for revised clause
3182	256	16.21 Annexure 21: Sizing/Volumetrics (gap for Offsite Services)	Annexure 21, Sizing table	Annexure 21's sizing table provides explicit volumetrics (EPS, endpoint counts, IPs, VPCs, etc.) for the 14 solutions under Section 7.3, but no equivalent executive/VIP count is specified for the offsite services that monitor executive exposure (Anti-Phishing - Cl. 7.4.5, Dark Web Monitoring - Cl. 7.4.6, Brand Protection - Cl. 7.4.9).	Cyble's Executive Monitoring and Digital Risk Protection capabilities can protect any number of the Bank's executives/VIPs from Day 1, with coverage scaled precisely to the Bank's requirement across Anti-Phishing, Dark Web Monitoring and Brand Protection. To finalise sizing, we request the Bank confirm the number of executives/VIPs (e.g., Board members, CXOs, senior management) to be brought under continuous monitoring at contract commencement.	Please refer to the relevant Addendum for updated specfications
3183	256	16.21 Annexure 21: Sizing/Volumetrics (gap for Offsite Services)	Annexure 21, Sizing table	As above - no domain/sub-domain count is specified for the offsite services that monitor the Bank's external digital footprint (Attack Surface Management - Cl. 7.4.3, Anti-Phishing - Cl. 7.4.5, Brand Protection - Cl. 7.4.9).	Cyble can bring any number of the Bank's domains and sub-domains under continuous monitoring across Attack Surface Management, Anti-Phishing and Brand Protection from Day 1. To finalise sizing, we request the Bank confirm the number of primary domains and sub-domains to be monitored at contract commencement, and the expected annual growth in this count.	details shall be shared with successful bidder

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3184	54	7.4 Functional Requirement - Services (Offsite Services)	Cl. 7.4(d)	"The Bidder shall implement appropriate security controls, including data masking or tokenization for sensitive data, Role-Based Access Control (RBAC), Just-in-Time (JIT) privileged access, and comprehensive audit logging for all services delivered under this RFP." - no named-user/license count is specified for platform/dashboard access to the 9 offsite services.	Cyble's platform can be provisioned for any number of the Bank's analysts, CISO-office and compliance stakeholders who need dashboard access to the offsite services, with full role-based access control as required under Cl. 7.4(d). To size the commercial bid precisely, we request the Bank confirm the number of named analyst/console user licenses required for the Bank's teams to access Cyble's platform and reporting for the proposed offsite services.	details shall be shared with successful bidder
3185	55, 58	7.4.5 Anti-Phishing / 7.4.9 Brand Protection and Monitoring	Cl. 7.4.5; Cl. 7.4.9(j)	Neither clause, nor Annexure 21, specifies an expected volume of takedown actions per month/year for phishing sites, fraudulent domains, or fake social media/mobile app listings.	Cyble is fully equipped to execute takedown actions at whatever volume the Bank's threat exposure requires. To align commercial terms precisely with the Bank's risk profile, we request the Bank confirm the estimated number of takedown actions (phishing sites, fraudulent domains, fake social media/mobile app listings) expected per month under Anti-Phishing and Brand Protection.	Please refer to the relevant Addendum for updated specfications
3186	103	10.2 - 6	Eligibility Evaluation Criteria		Bidder should have more than 100 manpower on payroll experience in ICT and out of which 50 cybersecurity employees on bidder payroll,	No Change, Please be guided by the RFP
3187		Cl. 20			BFSI/ large enterprise clients to eligible customer categories as Several of these are emerging/specialized technologies where references may exist in large enterprises rather than BFSI. Kindly permit equivalent enterprise references.	No Change, Please be guided by the RFP
3188	102		OEM Cl. 23		Permit experience in any 3 or 4 of the listed services, with the remaining services supported by OEM/service-provider credentials As:- The nine services include specialized services such as continuous automated red teaming, dark web monitoring and brand protection. Requiring a reference for every individual service may not be possible in single PO.	No Change, Please be guided by the RFP
3189	NA	NA	Additional Clause	To allow Bidder along with its affiliate including its subsidiaries to participate	Request department to allow 100% subsidiary as a bidding entity. Requesting credentials of the Parent Group entity and also its financial statements to be considered for the purpose of meeting the eligibility criteria. Request to include the below for allowing participation via wholly owned subsidiary/demerged entity while using the credentials of the parent company. "In case of corporate restructuring, demerger or hiving off from the parent organization, the parent organization's Incorporation certificate, Financial Statements, Pre-Qualification, Credentials, etc. will be considered for meeting the PQs & TQs" Refer attached Memorandum	No Change, Please be guided by the RFP
3190	NA	NA	Additional Clause	Terms & Conditions	Please confirm whether GeM or RFP terms & conditions will prevail	No Change, Please be guided by the RFP
3191	74	1788963158-RFP	7.12.2	O&M Phase Resource requirement:L1 req 2+ exp	Req 2 year experience, also written exp in SOC since last 5 years	No Change, Please be guided by the RFP
3192	75	1788963158-RFP	7.2.14		What is Customer working days (5 days or 6 days)	Please be gudied by the RFP, Support is to be provided 24x7x 365 basis
3193	75	1788963158-RFP	7.2.14		These resource count for DC or DR or for both to be distribute	The Resource requirement given in the RFP is minimum mandatory requirement that is to be deployed. It includes both DC & DR. Bidder can propose the manpower over and above if required.
3194	80	1788963158-RFP	7.13 Facilities Management	Bidder & OEMs should engage data scientists for analytics, statistical models, configuring the systems for supervised & unsupervised learning leveraging AI / ML to take over the activities of L1 & L2 resources by systems, minimizing the false positives and in developing advanced analytics use cases without any additional cost to the bank.	The Data Scientists would be part of onsite SOC team or Remote Resources? What is the frequency expected for review by Data Scientists?	The Data Scientists shall be part of the bidder/OEM's SOC support team. Bidder is required to right size and design the SOC Support team
3195	83	1788963158-RFP	7.13.1 Continual Improvement	36. Shifting of IT hardware within the premises, reinstallation and configurations including cabling and asset labelling.	Is this in SOC RFP Scope?	Yes, the requirement is within the scope of the SOC RFP, to the extent it relates to the proposed NextGEN SOC security infrastructure and hardware deployed or managed as part of the proposed SOC solution. The bidder shall be responsible for shifting, reinstallation, configuration, cabling and asset labelling of such SOC-related hardware, as and when required during deployment, relocation, upgrade, replacement or other activities associated with the implementation and operation of the proposed solution.
3196	84	1788963158-RFP	7.15 NextGEN SOC operations:	9. Perform fortnightly & monthly gap analysis of issues/threat/vulnerabilities in OS, databases, web servers, applications and devices and entire IT infrastructure & recommend and implement remedial actions.	Does bank have Vulnerability Management tool and is it expected to integrate the same which scan entire IT Infrastructure?	Bidder is required to propose the VA & VLM Tool as a part of the proposed NextGEN RFP
3197	Appendix 1A Page 40	NDR Functional Compliance Sheet	Clause 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high- availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	The Clause mandates Cloud based SaaS model, while RFP Page 30, Page 35, section 7.2.4.1 clause 'd' asks for on Premises solution "The NDR shall be deployed On-Premises". We request to modify the clause to include On-Prem solution. Justification: To include solutions which are on-Prem based	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3198	Appendix 1A Page 40	NDR Functional Compliance Sheet	Clause 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high- availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	The Clause asks for Active-Active HA architecture, we request to include Active-Standby Mode. Justification: Management Console is central console, it cannot be deployed in Active-Active mode, as it is a central component.	Please refer Addendum for revised clause
3199	Appendix 1A Page 41	NDR Functional Compliance Sheet	Clause 18	Solution should have the capabilities to create and run security playbooks for automation and better MTTD/MTTR on the basis of criticality of threat/server	Proposed solution adopts below approach for automated MTTD, Solution need investigative workflows and all the alerts need to be validated before building any Active Response Solution is having inbuilt playbooks like Host, Session and Packet analysis. once alert is validated Active Response can be triggered. Hope the approach is acceptable	Please refer addendum for the revised clause
3200	Page 66	7.6.7	Training	At a minimum, the following training programs shall be conducted for each proposed solution / OEM appointed officials: Duration per Session and Minimum Number of Sessions	Overall there is a requirement of 15 Sessions and Duration per session is 2 or 3 days. This takes the total training per solution to 40 days. This is very large requirement of training, we request to make it to 3 days for NDR solution	Please refer addendum for revised clause
3201	Page 63	7.6.6	Testing, clause 3	The bidder shall provision and maintain dedicated Development, Testing, UAT, and Pre-Production environments throughout the contract period.	Is UAT Environment required for NDR solution also, given that NDR is a Passive and out of path solution.	Please refer addendum for revised clause
3202	Page 143	13 SERVICE LEVELS & PENALTIES	13 SERVICE LEVELS & PENALTIES	Resolution SLA	As this RFP is about SOC for log monitoring, would resolution SLA be applicable as bidder will not manager any technology except SOC solution	No Change, Please be guided by the RFP. The Resolution SLA shall apply to the bidder's in-scope solution, tools, IT Infrastructure, and services as defined in the RFP and anything required to meet the terms of the RFP.
3203	Page 147	Services SLAs:		b. Site take-down time for identified Phishing URLs – Resolution within 24 hours c. Site take-down time for Brand Abuse – Resolution within 36 hours	The Site take down would depend on response from Register hence there is no defined resolution time. This need to exclude.	No Change, Please be guided by the RFP
3204	29-31	7.2.1:-	Deployment Matrix	Cloud SaaS + Hybrid HA Architecture	Please confirm whether management consoles deployed at DC and DR are required in active-active mode or active-standby mode.	Please refer addendum for the revised clause
3205	29	7.2.1	SIEM HA	Cloud(SaaS)+Hybrid HA N+N Active-Active	Request you to kindly confirm the SIEM solution is required as dedicated	No Change, Please be guided by the RFP
3206	36-38	7.2.4.3	Cloud Storage Retention	SIEM Retention	Please clarify whether 60 months retention for parsed logs is required online/searchable or can part of the retention reside in archive storage with retrieval on demand.	Pleae refer addendum for revised clause
3207	36	7.2.4.3	SIEM Retention	1 month raw, 60 months parsed logs	Can archived logs retained on Bank LTS(Long Term Storage) be stored in compressed OEM-native format, provided they remain searchable/restorable?	No Change, Please be guided by the RFP
3208	36	7.2.4.3	Cloud Backup	Backup to Bank infrastructure	Please clarify the connectivity mechanism and bandwidth responsibility for transferring backups from SaaS solutions to Bank backup storage.	The Bidder/OEM shall be responsible for defining the required connectivity mechanism for secure transfer of data, information, logs, backups and other required traffic between the SaaS environment and the Bank's DC and DR environments, and vice versa, as applicable to the proposed solution. The Bank has existing MPLS/Internet connectivity at its DC and DR locations.
3209	39	7.3.1.1	Modules, Architecture & Deployment:	4. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Please confirm whether integration with existing Bank MFA solution will be provided by Bank or bidder to arrange separate MFA solution and that can be integrable with BANK MFA solution.	The proposed solution shall, by default, provide native Two-Factor Authentication (2FA)/Multi-Factor Authentication (MFA) capability as an integral security feature. The solution shall also be capable of integrating with the Bank's existing MFA solution, if the Bank elects to use the Bank's existing MFA solution for authentication. Where such integration is required by the Bank, the Bank may provide necessary technical details or reasonable support for integration. The Bidder and OEM shall be responsible for ensuring compatibility, configuration and implementation of the required integration as part of their scope.
3210	39	7.3.1	SIEM Integration	Entire IT ecosystem integration	Please confirm whether integration of future systems added during contract period and OEM/ Bidders requires to develope parsers/connectors, then cost should be taken care by Bidder or Bank will take it separately because future expansion is not limited and unknow to development of parser.	No Change, Please be guided by the RFP
3211	40	7.3.1.1	6.Support collection of logs and telemetry from, at a minimum:	I) Third-party systems and services	Please clarify the no. of location of third party system, is it same as per bank location. And number of third party services with hosted location i.e. (Op-prem/SaaS).	The Bidder/OEM shall clearly identify in its technical proposal all third-party systems, services, OEM platforms, cloud/SaaS services and subprocessors proposed or required for delivery of the solution
3212	49	7.3.10	AST	DAST/SAST enterprise	Please confirm whether unlimited scans include CI/CD-triggered automated scans.	No Change, Please be guided by the RFP
3213	45	7.3.6	Decoy	200 applications/networks/devices	Kindly confirm no. of applications required for Decoy.	Please refer addendum for revised clause
3214	258	Annexure 21	Decoy	50 segments	Please provide indicative count of VLANs/subnets where deception assets are expected to be deployed.	Please refer addendum for revised clause.
3215	258	Annexure 21	NDR	10 Gbps throughput	Please clarify whether NDR throughput requirement is aggregate or per location i.e. DC and DR.	Please refer addendum for the revised clause
3216	92-96	Appendix 1C	Brand Protection	Brand Protection	Please confirm the no. of Domains and Sub-domain to be considered for Brand Monitoring.	Details shall be shared with successful bidder
3217	92-96	Appendix 1C	Brand Protection	Brand Protection	kindly confirm the no. of social media sites need to be consider(FB, LinkIN etc.)	Details shall be shared with successful bidder
3218	92-96	Appendix 1C	Brand Protection	Brand Protection	Does the bidder needs to consider Executine Monitor.	Yes, Your understanding is correct
3219	54-58	Services	Threat Hunting	Continuous service	Kindly confirm the no. Log Days to be consider for Threat hunting.	The Bidder shall ensure that the proposed Threat Hunting service is capable of searching, correlating and analysing the available historical data within the applicable retention period.
3220	45-59	TIP	Threat Intelligence	Feed integration	Kindly confirm does the Bank have existing Threat Intell feed that need to be integrated with the proposed SIEM solutions	The Bidder/OEM shall provide the required Threat Intelligence Feeds as part of the proposed solution, including the necessary subscriptions, integrations and updates throughout the contract period.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3221	45-59	TIP	Threat Intelligence	Feed integration	Does the bidder need to provide multiple threat Intel platform bundle with solution.	No Change, Please be guided by the RFP
3222	84-86	SOC Operations	Use Cases	15 use cases per application	Please clarify the count of business applications for which dedicated use cases are expected.	Details shall be discussed with succesfull bidder
3223	258-260	Volumetrics	SOAR	Unlimited actions	Please confirm expected daily incident volume and automation execution volume for sizing.	No Change, Please be guided by the RFP
3224	Page 168	Section 14.24	Audit by Third party	Audit by Third party	Bidder suggests that appropriate prior notice for at least 30 days to be given to Bidder before any such audit / inspection is conducted by the Bank or its appointed auditors and such audit shall be conducted at the Customer's sole cost and expense. This audit shall be conducted annually only for the services provided by Bidder.	No Change, Please be guided by the RFP
3225		GEM Bid Document		MII Compliance: Yes	Request relaxation on MII compliance	No Change, Please be guided by the RFP
3226		GEM Bid Document		Purchase Preference to MSE OEMs/ Service Provider available upto price within L1+15%	Request relaxation, all bidders should be evaluated equally without price preference for MSE.	No Change, Please be guided by the RFP
3227			Additional Clause	Subsidiary/Affiliate	Kindly confirm that Bidder along with its affiliate including its subsidiaries shall participate in the bid. The contracting and invoicing for proposed services/goods specified in this RFP will be managed by bidder or its wholly owned subsidiary. Please confirm	No Change, Please be guided by the RFP
3228	98	8 CONTRACT PERIOD	8 CONTRACT PERIOD	The bank may, at its sole discretion, extend the contract for an additional period of two years, in one-year increments tranches. The Bank may extend the support services for an additional period of up to two (2) years beyond the original contract period. The pricing applicable during the extension period shall be mutually agreed and shall not exceed 120% of last year's AMC/ATS/Facility management rates quoted by the Selected Bidder. The decision to further extend the contract with the same bidder shall be at the sole discretion of the Bank. Further, the Bank will have the right to renegotiate prices of AMC, ATS, Facility Management rates at the end of the contract period.	Extension of contract post 5 year term and the prices should be mutually agreed during renewal. Bidder wont be able commit on prices post 5 year contract term. OEM cost can change, hence prices for contract extension period should be as per mutual agreement reflecting market rates. Request relaxation on this clause.	No Change, Please be guided by the RFP
3229	98	8 CONTRACT PERIOD	8 CONTRACT PERIOD	End of Sales / End of support: The bidder must ensure that any equipment (hardware/software) supplied as part of this RFP should not have either reached or announced end of sales as on the date of such supply or end of support for at least duration of the contract (including the period of 2-year extension).	Request relaxation, OEMs wont give commitment of EOS for 7.5 years from now. Request to limit this to duration of contract term, 5 years.	Please refer addendum for revised clause.
3230	136	11 Right to Reduce / Descope Solution Components Prior to Award	11 Right to Reduce / Descope Solution Components Prior to Award	The Bank reserves the right, at its sole discretion and in the interest of economy, optimization of requirements, technological suitability, or business/operational necessity, to accept, reject, reduce, modify, defer, or descope - one or more Solution Components, Modules, Licences, Services, Quantities, or associated IT Infrastructure items forming part of the scope of this RFP, at any stage prior to issuance of the Contract/Letter of Award.	Request to ensure order is placed as per quantity in solution BoQ, as price can change in case reduction in quantity	Please refer the addendum for revised clause
3231	165	13.19 Liquidated Damages	13.19 Liquidated Damages	If the bidder fails to deliver any or all of the products, systems and services solutions within the time period(s) specified in the Delivery Schedule or installation, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 0.5 percent per week or part thereof of Contract Price subject to maximum deduction of 10% of the total contract value, until actual delivery, installation or performance as per related clauses mentioned in RFP.	LD Penalty of 0.5% per week is on the undelivered portion of product/ service, please confirm? Will penalty be on undelivered portion of ACV or TCV?	No Change, Please be guided by the RFP
3232	166	14.22 Order Cancellation	Termination for convenience	Bank's Right to terminate the entire/ unexecuted part of the Purchase Order on Convenience 1) The Bank reserves its right to cancel the entire unexecuted part of the Purchase Order at any time on its convenience without assigning any reason/s whatsoever. 2) In the event of termination of the Agreement for the Bank's convenience, bidder shall be entitled to receive payment for the Services rendered (delivered) up to the effective date of termination.	Request relaxation to exclude termination for convenience. Bidder will have to pay suppliers for Hardware/ Software/ AMC/ ATS for entire contract term. This clause will have significant commercial risk to bidder. In case customer terminates for convenience, Early termination charges for the remainer period should be paid to bidder.	No Change, Please be guided by the RFP
3233	72	7.11 Warranty, ATS and AMC	7.11 Warranty, ATS and AMC	The rates quoted by the bidder for hardware, software, licenses, subscriptions, ATS, AMC, and related services shall remain applicable on a pro-rata basis for any additional quantities or services procured by the Bank during the contract period.	Prices can change based on market prices within 5.5 years contract term. TCL cant agree for price protection for incremental orders as OEMs wont provide any cost protection.	No Change, Please be guided by the RFP
3234	7	1 KEY INFORMATION	1 KEY INFORMATION	180 days from the date of opening of the bid.	Request bid validity to be reduced to 30 days due to fluctuating CPE prices based on present Geopolitical situations.	No Change, Please be guided by the RFP
3235	137	11 PAYMENT TERMS	11 PAYMENT TERMS	Product License Cost Payment Schedule	Request to relax, payment to be offered one time in advance, net 30 days	No Change, Please be guided by the RFP
3236	137	11 PAYMENT TERMS	11 PAYMENT TERMS	Subscription Cost (One time license Cost)	Request to relax, payment to be offered 100% on license activation.	No Change, Please be guided by the RFP
3237	138 & 139	11 PAYMENT TERMS	11 PAYMENT TERMS	Hardware Cost including appliance	Request to relax, payment to be offered 100% on Hardware delivery.	No Change, Please be guided by the RFP
3238	139	11 PAYMENT TERMS	11 PAYMENT TERMS	ATS/ Annual Subscription & Appliance AMC Cost	Request to relax, payment to be offered, one time in advance for 5-year support.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3239	261	Deployment and Data Retention	Retention Requirement		Please confirm if the Long Term Storage is inclusive of the back Up storage	The Bidder/OEM shall assess the workload, application architecture, data growth, performance requirements, backup requirements, retention requirements and other relevant parameters of the proposed Security Solution and shall accordingly design, size and propose the complete storage infrastructure. The storage infrastructure shall comprise, at a minimum, the following: **a) Primary Storage – Hot Storage:** Storage for hosting the active/production workloads of the Security Solution, as required by the solution architecture. **b) Backup Storage / Backup Appliance:** Dedicated storage/backup appliance for receiving and managing backups of the Security Solution. The Bidder/OEM shall ensure that the proposed backup infrastructure is appropriately sized to meet the required backup window, recovery requirements, performance and capacity requirements. **c) Long-Term Storage: - Cold Storage** Dedicated storage for retaining backup data for the stipulated retention period/contract duration. This storage shall be used exclusively for backup data and shall be connected to the backup infrastructure. It shall not be proposed as
3240	37	7.2.4.3 Storage and other Requirement	Primary Log Storage & Retention	Parsed, normalized, enriched, indexed and correlated logs, together with associated metadata and contextual information, shall be retained for a minimum period of 60 months (5 years).	Please clarify if the bank will provide the network connectivity and egress charges for the logs to be pushed from the CSP to LTS at the Bank's Dc & DR locations	The bidder shall support complete and usable extraction/ transition of Bank-owned data required for continuity, regulatory, audit and exit purposes. Data shall be provided in industry-standard, documented, machine-readable/native formats, as applicable to the solution. The bidder shall not impose artificial technical restrictions on extraction. The Bank may specify a transition plan and data set during exit. All required ingress/egress cost is part of the bidder's scope Also, Please refer addendum for the revised clause
3241	110		OEM Evaluation Criteria		We request the Authority to kindly clarify whether successful implementation and management/maintenance of the proposed OEM SIEM solution in a Government/PSU/Central Government organization in India, with a capacity of 30000+ EPS on an on-premise deployment, may be considered against the stipulated SIEM experience criteria. We further request clarification on whether on-premise SIEM implementation experience meeting the specified capacity requirement may be accepted in lieu of the mandatory cloud implementation experience. Justification: Justification: The technical capabilities of SIEM, including event collection, correlation, security monitoring, alert generation and analysis, are fundamentally applicable across different deployment environments. Therefore, restricting the experience specifically to BFSI and cloud deployments may unnecessarily limit participation despite equivalent technical and operational experience. Hence, we request the Authority to kindly consider Government/PSU/Central Government experience and on-premise SIEM implementation experience meeting the specified capacity as equivalent and acceptable for compliance with the eligibility criteria.	The bidder shall not impose artificial technical restrictions on extraction. The Bank may specify a transition plan and data set during exit.
3242	112		OEM Evaluation Criteria		The tender requires the proposed OEM solution to have been implemented in at least one BFSI organization in India for the following solutions: SOAR, UEBA, XDR, NDR and Threat Intelligence Platform. We request the Authority to kindly clarify whether successful implementation experience in Government/PSU/Central Government organizations or other large enterprises in India may be accepted in lieu of the BFSI-specific implementation experience. Justification: The proposed solution complies with the specified technical requirements for SOAR, UEBA, XDR, NDR and Threat Intelligence Platform. However, restricting the implementation experience specifically to the BFSI sector may limit participation of OEMs having proven cybersecurity capabilities and deployments across other critical sectors. Government, PSU and Central Government organizations also operate critical IT infrastructure and face complex cybersecurity threats, requiring capabilities such as security orchestration, behavioural analytics, extended detection and response, network detection and threat intelligence.	No Change, Please be guided by the RFP
3243					Sr. No. Justification: Page No.	All required ingress/egress cost is part of the bidder's scope
3244					A.1 Justification: --	No Change, Please be guided by the RFP
3245	Page No.	Section	RFP Clause	Clause / Technical Specification	Bidder's Query	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3246	7	KEY INFORMATION	Security Deposit/Earnest Money deposit	Rs. 4.25 Crore (INR Four Crore and Twenty-Five Lakh Only) Note: - Bidders who are eligible for EMD (Earnest Money Deposit) exemption as per GeM General Terms and Conditions (GeM 4.0, Version 1.25, dated 14th July 2025, Page 19) are required to submit a Bid Security Declaration in lieu of EMD. Please refer to RFP, Annexure 4: Bid Security Declaration for the prescribed format. This declaration must be duly filled, signed, and submitted along with the bid documents by vendors seeking the waiver of EMD submission. Failure to submit the Bid Security Declaration (where applicable) will result in the bid being treated as non-responsive.	We request the Authority to kindly confirm whether bidders who are eligible for EMD exemption under the applicable GeM provisions as on the date mentioned above shall be permitted to participate in the tender without submitting the EMD of ₹4.25 Crore, subject to submission of the prescribed Bid Security Declaration as per Annexure 4 of the RFP. Further, kindly confirm that submission of the duly signed Bid Security Declaration shall be considered sufficient compliance with the EMD requirement for such eligible bidders and that their bids shall not be treated as non-responsive solely on account of non-submission of the EMD.	No Change, Please be guided by the RFP
3247	101	Eligibility Evaluation Criteria	10.2, Eligibility Evaluation Criteria	The bidder should have a minimum average turnover of INR 500 crore per annum in India during the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth.	The bidder should have a minimum average turnover of INR 400 crore in India during the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth.	No Change, Please be guided by the RFP
3248		Additional Clause		The RFP specifies an Earnest Money Deposit (EMD) of ₹4.25 Crore. We request the Authority to kindly consider and permit submission of an Insurance Surety Bond (ISB) issued by an IRDAI-registered insurance company as an acceptable instrument towards the EMD requirement. Acceptance of an Insurance Surety Bond would provide bidders with an additional permissible mode of furnishing the required bid security and would facilitate wider participation in the tender. We therefore request the Authority to kindly confirm whether bidders may submit an Insurance Surety Bond for ₹4.25 Crore, in the prescribed format and validity as specified in the RFP, in lieu of the EMD.	Please clarify that Insurance Surety Bond shall be accepted as an eligible mode of submission of EMD for the tender,	Please refer addendum for the revised clause
3249	192	Eligibility Evaluation Criteria	10.2, Eligibility Evaluation Criteria	Proposed OEM SIEM solution ≥30,000 EPS or 1.2 TB/day successfully implemented and under management/maintenance in at least one BFSI in India; also successfully implemented on cloud in one India deployment. Client PO/WO/Contract + client supporting document + OEM self-declaration	OEM SIEM solution ≥30,000 EPS or 1.2 TB/day successfully implemented and under management/maintenance in at least one BFSI in India; also successfully implemented on cloud or Hybrid in one organisation Globally	Please refer addendum for revised clause.
3250			7.2.1	SIEM, SOAR and UEBA are explicitly required as Cloud (SaaS) + Hybrid solutions, not pure on-premises deployments.	SIEM, SOAR and UEBA are required as Cloud (SaaS) or Hybrid Solutions Deployment	Please refer addendum for the revised deployment architecture
3251	136	12.4	Payment Terms	Annually in Advance: Upon submission of a Bank Guarantee equivalent to 110% of the annual subscription/Annual technical cost of the respective product, valid for the applicable subscription period; or Quarterly in Arrears	As per prevailing industry/OEM policy, the ATC/subscription charges are generally payable in advance. However, PSB has stipulated payment on a quarterly-in-arrears basis. This payment structure will adversely impact the bidder's cash flow and may result in additional financing costs, which would ultimately increase the overall bid price. Alternatively, if a bidder opts for advance payment by providing an additional PBG, the associated financial and administrative costs would again increase the project cost. Moreover, PSB is already requiring a PBG under the tender conditions. In view of the above, we request the Department to kindly reconsider and remove the Advance BG clause. This will reduce the additional financial burden on bidders, avoid unnecessary financing costs, and encourage wider participation, thereby making the bid more competitive and cost-effective for PSB. We request the Department to kindly consider this amendment in the interest of healthy competition and optimal pricing.	No Change, Please be guided by the RFP
3252			Price Bid Formet	Product License Cost	We request the Department to kindly clarify where the Bidder should quote the price for the cloud-based license/subscription, as OEMs generally offer such licenses on a monthly, quarterly, or annual subscription basis. Further, the RFP specifies a warranty period of 3 years. In this regard, kindly clarify whether the Bidder is required to quote the complete 3-year license/subscription cost upfront under the Product License Cost Sheet, or whether the license cost is to be quoted based on the OEM's applicable subscription billing cycle. Clear guidance on the above will help bidders ensure uniformity in their commercial quotations and avoid any ambiguity in the evaluation of the bids.	The pricing shall be provided in the two separate sheets provided in the BOM/pricing template: Product License Cost: The bidder shall quote the applicable one-time perpetual license cost or initial subscription cost, as applicable, for the respective products/solutions. The relevant product/license details shall be provided in this sheet. ATS / Annual Subscription Cost: The bidder shall quote the applicable Annual Technical Support (ATS) / Annual Subscription Renewal Cost in the sheet provided for Y1 to Y5, post Go-Live. The bidder shall clearly identify the applicable licensing model (Perpetual/Subscription) for each product/solution and ensure that there is no duplication between the Product License Cost and ATS/Annual Subscription Cost. The BOM/pricing format remains unchanged.
3253	21	PBG	6.11 sub-clause 9	Cure period mentioned as 30 days	cure period of 30 60 days would be viable.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3254	141	Service Levels & Penalties	Clause 13 sub clause 13.1(8)	Failure to provide support services in accordance with the SLA requirements, including the required support coverage and service quality specified in this RFP, may result in bank levying penalty, termination of the contract, or any other action deemed appropriate by the Bank, without prejudice to its other contractual rights and remedies.	We propose to modify the clause:- Failure to provide support services in accordance with the SLA requirements, including the required support coverage and service quality specified in this RFP, the Bidder be provided with a cure period of 30 days to remedy the defects/deficiency. However, if the Bidder fails to rectify the defects/deficiency within the cure period, then the Bank may levy penalty at the rate of ___ (of the total contract value), termination of the contract, or any other action deemed appropriate by the Bank, without prejudice to its other contractual rights and remedies.	No Change, Please be guided by the RFP
3255	159	Terms and Conditions	Clause 14 sub clause 14.1(2)	If the Bank undergoes a merger, amalgamation, takeover, consolidation, reconstruction, change of ownership, etc., this tender shall be assigned to the new entity, and such an act shall not affect the rights of the Agency under this tender.	We propose to modify the clause:- If the Bank undergoes a merger, amalgamation, takeover, consolidation, reconstruction, change of ownership, etc., this tender shall be assigned to the new entity, and such an act shall not affect the rights of the Bidder under this tender. Also, the new entity shall be bound by the terms of the SLA, NDA and all the agreements/contracts entered into by and betweeen the Bank and the Bidder, as if the same has been entered into by and between the new entity and the Bidder.	No Change, Please be guided by the RFP
3256	159	Terms and Conditions	Clause 14 sub clause 14.2	The bank reserves the right, at the time of award of contract and/or during the currency of the contract, to increase or decrease the quantity of goods, licenses, subscriptions, appliances, equipment, services, implementation effort, support services, or any line item covered under the contract by up to twenty-five percent (25%) of the quantities specified in the RFP/Contract, without any change in the unit prices, terms and conditions, technical specifications, delivery schedule, warranty obligations, support commitments, or any other contractual conditions.	We propose to modify the clause:- The bank reserves the right, at the time of award of contract and/or during the currency of the contract, to increase or decrease the quantity of goods, licenses, subscriptions, appliances, equipment, services, implementation effort, support services, or any line item covered under the contract by up to ten percent (10%) of the quantities specified in the RFP/Contract, without any change in the unit prices, terms and conditions, technical specifications, delivery schedule, warranty obligations, support commitments, or any other contractual conditions. Also, the Bank will notify the Bidder by a ten days (10) prior written notice before changing the quantities of any of the above listed services/goods/materials.	No Change, Please be guided by the RFP
3257			-	Legal Query	We reccomend to add below clause under the RFP:- Termination by the Bidder for breach:- In the event BSNL materially breaches this definitive Agreement or any statement of work, which breach is not cured within thirty (30) days after written notice specifying the breach is given to the BSNL, the Contractor may terminate this defenitive Agreement or any portion thereof or the applicable statement of work by giving written notice to the BSNL.	No Change, Please be guided by the RFP
3258			-	Legal Query	We recommend to incorporate a new clause under the RFP, which shall be mutually beneficial and significant in the context of business engagements Non-Solicitation:- During the Term of this definitive Agreement and for a period of one year thereafter, neither Party shall (either directly or indirectly through a third party) solicit to employ, cause to be solicited for the purpose of employment to any employee/s (including the employees who have been exposed or introduced to other Party during initial discussion between Parties or engaged to provide/perform the services under any definitive agreement entered between Parties) of the other Party or aid any third person to do so, without the specific written consent of the other Party. The said restriction shall also apply to each Party's affiliates, agents, vendors, contractors, and any third parties with whom such Party has a relationship (collectively, "Representatives"). Parties agree that Representatives are equally restricted from poaching or soliciting or inducing any employees of other Party to leave their employment or engagement with such other Party.	No Change, Please be guided by the RFP
3259			Functional Specification	The proposed solution shall support dynamic log parsing and normalization upon ingestion. In cases where historical security telemetry must be re-parsed, re-processed, or re-modeled using updated parsing rules or processing logic, the platform shall provide high-speed, cloud-native mechanisms to re-process retained historical telemetry using the updated parsing and processing logic, without impacting active SOC performance, availability, or operational detection capabilities.	The proposed solution shall support dynamic log parsing and normalization upon ingestion. In cases where historical security telemetry must be re-parsed, re-processed, or re-modeled using updated parsing rules or processing logic, the platform shall provide high-speed, cloud-native/hybrid mechanisms to re-process retained historical telemetry using the updated parsing and processing logic, without impacting active SOC performance, availability, or operational detection capabilities.	No Change, Please be guided by the RFP
3260			Functional Specification	The proposed solution shall be scalable and shall provide a cloud-native, highly available architecture with built-in redundancy and service continuity. The solution shall provide continuous security monitoring through cloud-native high availability and disaster recovery capabilities, with a minimum uptime commitment of 99.9%	The proposed solution shall be scalable and shall provide a cloud-native/hybrid highly available architecture with built-in redundancy and service continuity. The solution shall provide continuous security monitoring through cloud-native/hybrid high availability and disaster recovery capabilities, with guaranteed High availability/Redendency	No Change, Please be guided by the RFP
3261			Functional Specification	The proposed solution shall provide cloud-native high availability and redundancy mechanisms to tolerate failures of underlying infrastructure components without disruption to security monitoring and operational capabilities. The solution shall provide automated failover and service continuity within the cloud environment through the CSP's native availability and resiliency capabilities	The proposed solution shall provide cloud-native/hybrid high availability and redundancy mechanisms to tolerate failures of underlying infrastructure components without disruption to security monitoring and operational capabilities. The solution shall provide automated failover and service continuity within the cloud environment through the CSP's native or Hybrid solution's availability and resiliency capabilities	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3262			Functional Specification	The proposed cloud-based solution shall support flexible data representation and analysis by enabling multiple views, schema interpretations, and query-time transformations of the same collected data without requiring redundant data storage or unnecessary reprocessing. The cloud platform shall support creation of customized searches, dashboards, and reports based on business and security monitoring requirements.	The proposed cloud-based/hybrid solution shall support flexible data representation and analysis by enabling multiple views, schema interpretations, and query-time transformations of the same collected data without requiring redundant data storage or unnecessary reprocessing. The cloud/hybrid platform shall support creation of customized searches, dashboards, and reports based on business and security monitoring requirements.	No Change, Please be guided by the RFP
3263			Functional Specification	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	The proposed solution shall feature a cloud-native SaaS/Hybrid console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud/hybrid architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	Please refer Addendum for revised clause
3264			Functional Specification	The proposed cloud-delivered solution shall provide appropriate encryption, tenant isolation, secure authentication, MFA, RBAC, audit logging and protection of Bank security data in accordance with the applicable service architecture and SLA.	The proposed cloud-delivered/hybrid solution shall provide appropriate encryption, tenant isolation, secure authentication, MFA, RBAC, audit logging and protection of Bank security data in accordance with the applicable service architecture and SLA.	No Change, Please be guided by the RFP
3265			UEBA	The proposed solution shall support dynamic log parsing and normalization upon ingestion. In cases where historical security telemetry must be re-parsed or remodeled under updated processing logic, the platform must provide high-speed, cloud-native ingestion pathways to re-ingest and re-process the historical log streams within the SIEM/platform repository without impacting active SOC performance, availability, or operational detection engines.	The proposed solution shall support dynamic log parsing and normalization upon ingestion. In cases where historical security telemetry must be re-parsed or remodeled under updated processing logic, the platform must provide high-speed, cloud-native/hybrid ingestion pathways to re-ingest and re-process the historical log streams within the SIEM/platform repository without impacting active SOC performance, availability, or operational detection engines.	No Change, Please be guided by the RFP
3266			UEBA	The proposed solution is a fully managed, cloud-native SaaS platform that guarantees 99.9% uptime	The proposed solution is a fully managed, cloud-native SaaS/Hybrid platform that guarantees High availability/Redendency	No Change, Please be guided by the RFP
3267			UEBA	The proposed solution shall feature a cloud-native SaaS delivery model that secures cloud workloads and hybrid SaaS environments through a single cloud console	The proposed solution shall feature a cloud-native SaaS/hybrid delivery model that secures cloud workloads and hybrid SaaS environments through a single console	No Change, Please be guided by the RFP
3268		Appendix 1A Functional Compliance Sheet (Solutions) CTEM	8	The solution should allow messaging and collaboration within the context of a specific intelligence item	We understand that this scope is for the bidder to collaborate on incidents/alerts within the team.	Please refer the below clarification: Example: CVE is found in multiple endpoints/devices then it should be contextualized and integrate with SIEM for Incident creation The System should provide access to relevant team and share RBAC intelligence
3269			24	The solution should provide pre-built bidirectional integrations with SIEM, SOAR, ticketing (Manage Engine), and threat intelligence platforms	We understand that the bidder will share the data with various on-premises tools like SIEM, SOAR, and ticketing tools (ManageEngine); hope this meets your requirement.	Please refer addendum for revised clause
3270			31	The solution should display a Security Score overview with full breakdown by issue category	Can the bidder provide the risk rating of the organization? We hope this will suffice the requirement.	Yes, Solution Need to provide Risk Rating on the Infrastructure.
3271			CTEM item 35	The solution should detect malicious files, reconnaissance activity, automated attack tools, and target lists	We understand that the bidder can achieve this functional requirement using a combination of tools like SIEM, SOAR, and other SOC components.	Please refer addendum for revised clause
3272			43	The ML model should continuously study the environment including asset relationships, topology, and security controls to detect false positives and identify root causes	We understand that the bidder can achieve this functional requirement using a combination of tools like SIEM, SOAR, UEBA, and other SOC components like TIP or EDR.	Yes, Understanding is correct
3273			48	The solution should assess and harden network, endpoint, and operating system security controls	We understand that the bidder can achieve this functional requirement using a combination of tools like SIEM, SOAR, UEBA, and other SOC components like TIP or EDR, including the day-to-day operations of SOC analysts.	Please refer addendum for the revised clause
3274			51	The solution should apply virtual patching/compensating controls/exposure mitigation mechaism to the firewall and other security systems through integration with relevant security controls.	We understand that the bidder can take preventive measures on other solutions, either manually or automatically using SOAR, based on the findings received from the CTEM solution.	Please refer addendum for the revised clause
3275			62	The solution should leverage compensating controls and layered defense strategies to manage threats proactively	We understand that this requirement can be achieved by the bidder through analysts managing the SOC during their day-to-day operations.	Please refer addendum for revised clause
3276		Appendix 1A Functional Compliance Sheet (Services) ASM	3	Solution should store historical information about bank to provide cybersecurity maturity over time	We understand that bank requires solution to store a detailed/ historical information on the detections and the attacks which were targeted on during the complete contract duration.	Yes, Your understanding is correct
3277			24	The solution must allow the organization to define the prioritization of assets based upon impact of the asset	We undestand that bank requires special attention/priortization to specific assests, so the bank can take preventive measures/ obseravility on it, it may be like assigning tags to certain important tags and creating a dashboard for critical ones.	Yes, your understanding is correct
3278			26	Solution must provide a workflow to define and manage state of discovered entities which affects the priority of the entity.	We understand that bank requires the solution to enable workflow for alerting the adminsitrators for any vulnerability detection on the discovered critical assests.	Yes, your understanding is correct

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3279			35	Solution should have the feature to automatically create help desk ticket containing asset meta data, comments, link back to the solution console and guidance. Ticket status should be automatically reflected in ASM console.	Please amend the clause as: Solution should have the feature to automatically create help desk ticket containing asset meta data, comments, link back to the solution console and guidance. Justification: We want authorities to clarify this, as we understand that bank requires ASM console to create tickets automatically for the detections and analysts to work upon?	Please refer addendum for the revised clause
3280			38	Solution must have bi-directional, writetable API's that allow the organization to integrate data into the organization's existing security	Please amend the clause as: Solution must have API's that allow the organization to integrate data into the organization's existing security Justification: since its services scope which is used to provide the outside attack surface details not the TIP Functionality so bidirectional API are not part of it.	Please refer addendum for the revised clause
3281		Appendix 1A Functional Compliance Sheet (Services) Brand Abuse	25	The Bidder should provide for identification of fake recruitment schemes claiming affiliation with the Bank	We understand that bank requires solution to provide for identification of fake recruitment schemes claiming affiliation with the Bank which has the bank names and logo or any other identification method	Please refer addendum for revised clause
3282			33	Search engines (like Google, yahoo, bing etc.) listing frauds where the customer care number & branch address of banks is changed/ modified should be continuously tracked and the same should be brought down immediately including True caller and JustDial.	Please delete this cluase its oem specific. Please modify the clause as to make it vendor neutral: Monitoring all major mobile app marketplaces for counterfeit, copycat apps, or apps infringing trademarks	Please refer addendum for the revised clause
3283			37	Bidder should be able to identify and report to the bank if access to blocked ports on a webserver is sought by an external user.	We understand that the ask is not resticted to Brand abuse solution bidder can achive this requirenment with the combination of multiple solutions as it would also requires logs from perimeter and application security solutions, its is part of SIEM Solution.	Please refer addendum for the revised clause
3284		Appendix 1A Functional Compliance Sheet (Services) Dark Web Monitoring	21	Monitor suspicious SSL/TLS certificate issuance.	We understand that bidder can achive this requirenement from either services product like ASM, Brand abuse or TI, this ask is not restrcited to DWM. As functional requirenment of bank is achieved anyways.	Yes, Understanding is correct
3285			25	Provide Passive DNS intelligence and historical DNS resolution.	We understand that bank requires DNS intelligence and bank wants the bidder to store the historical logs/analysis of the DNS specific abuse.	Yes, your understanding is correct
3286			40	Monitor C2 infrastructure, malware hosting, phishing infrastructure and botnets.	We undertand that bank requires information about the fake webistes which impersonating as PSB to Monitor C2 infrastructure, malware hosting and phishing infrastructure and botnets.	Yes, your understanding is correct
3287			44	Support Email, SMS, and other notifications based on configurable severity.	We understand that bidder can achive this requirenment by combination of multiple products to achive this functionality spcifically ITSM.	Yes, your understanding is correct
3288				clarifications	Please clarify: Does the solution have an established threat intelligence capability with more than 8 years of experience in global threat intelligence collection, analysis and threat actor tracking?	No Change, Please be guided by the RFP
3289				clarifications	Please clarify: Does the solution leverage intelligence from a global network of 400+ threat researchers, analysts and threat hunters?	No Change, Please be guided by the RFP
3290				clarifications	Please clarify: Does the solution collect and analyze threat intelligence across 14+ languages and sources?	No Change, Please be guided by the RFP
3291				clarifications	Please clarify: Does the solution provide threat intelligence derived not only from network and publicly available sources, but also from active monitoring, engagement and communication with relevant threat actor groups and underground communities to identify planned attacks, emerging campaigns, TTPs, compromised assets and indicators of compromise?	No Change, Please be guided by the RFP
3292				clarifications	Please clarify: Does the solution provide actionable threat intelligence on threat actor groups and campaigns, including their objectives, targeting, attack methods, TTPs, infrastructure and intended victims, along with recommended mitigation and protection measures to help the organization proactively defend against such threats?	No Change, Please be guided by the RFP
3293		Appendix 1A Functional Compliance Sheet (Services) Threat Hunting	3	Create use-cases correlation rules specific to client's environment and event sources.	We understand that the bidder can achieve this functional requirement using a combination of tools like SIEM, SOAR, UEBA, and other SOC components like TIP or EDR, including the day-to-day operations of SOC analysts. OEM, Services do not directly perform detection engineering. We however provide recommendations on identified gaps in detections	No Change, Please be guided by the RFP
3294			9	Review effectiveness of SOC to detect similar events..		No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3295			13	Threat Hunting shall also address the following If the SOC has detected the attack, then identify the reasons for no action being taken if the SOC has not detected the attack, then identify if an existing correlation rule requires tuning or if a new correlation rule is required or if a new solution is required.		No Change, Please be guided by the RFP
3296				clarifications	Since RFP Ask for the Threat hunting servcies from OEM but does not define the no of hours: Please clarify that the solution should be sized on the below: Vendor shall propose a 200-hour package to start with along with per hour cost and Bank shall decide to extend the number of hours depending on scope expected	No Change, Please be guided by the RFP Refer Section 7.2.2 Services
3297				clarifications	Please clarify: Does the proposed service provide organization-wide ransomware readiness and threat hunting across the complete security ecosystem, including infrastructure/products, people and processes, to proactively identify ransomware-related risks, vulnerabilities, attack paths, indicators and gaps, along with recommended remediation actions?	No Change, Please be guided by the RFP. The requirement shall be interpreted in accordance with the scope and functionalities specified under Section 7.4.8 – Threat Hunting Services, Appendix 1C. The Threat Hunting Service is intended to provide proactive, hypothesis-driven and intelligence-led technical threat hunting across the Bank's IT and security ecosystem. The service may utilize relevant telemetry and logs available through the Bank's SIEM, as well as other applicable security technologies and data sources, for identifying known and unknown threats,
3298				clarifications	Please clarify: Does the proposed service provide a comprehensive maturity assessment with a defined maturity rating and actionable recommendations to strengthen the overall cybersecurity program, prioritize security initiatives and investments, and improve business continuity, resilience and recoverability during unexpected cyber incidents?	No Change, Please be guided by the RFP
3299				clarifications	Please clarify: Does the proposed service provide a modular cybersecurity assessment and incident-readiness package offering, at a minimum, the following capabilities as per organizational requirements: SOC Gap Assessment, Ransomware Assessment, Forensic Analysis, Compromise Assessment, Incident Response Readiness Assessment, Active Directory Security Assessment, Tabletop Exercises, and Incident Response Playbook Development?	No Change, Please be guided by the RFP
3300		Appendix 1A Functional Compliance Sheet decoy	20	Includes an algorithm for automated rule creation that integrates with SOAR platforms, enabling real-time blocking of attacker IPs based on threat intelligence gathered from decoys. Features a customizable Generative AI model to assist security analysts with contextual insights, investigative support, and proactive security measures.	Please amend the clause as: Includes an algorithm for automated rule creation that integrates with SOAR platforms, enabling real-time blocking of attacker IPs based on threat intelligence gathered from decoys. Justification: GenAI is a functaionlity of soar solution where SOAR can create and run the playbook as per the event or alert where decoy is reponibsle for redirecting the attacker to fake vm to monitor the actvitites.	Please refer addendum for revised clause
3301			25	The proposed solution shall be delivered as a cloud-based/SaaS platform hosted within the CSP environment. The bidder shall provision and size the required cloud compute, storage, network, and other platform resources to meet the Bank's performance, scalability, High Availability (HA), service continuity, and Disaster Recovery (DR) requirements in accordance with the applicable Cloud Deployment Model.	Please amend the clause as: Proposed Solution must cover complete scope of min of 200 applications, networks, devices with 50 segments across DC-DR and capability to add additional decoy connector through decoy customization as per requirement Justification: Request to amend the requirement to allow an on-premises Deception Solution instead of a cloud-based solution, as cloud-based redirection of decoy traffic may introduce latency and dependency on WAN/Internet connectivity, impacting real-time attacker engagement and the overall effectiveness of deception.	Please refer addendum for revised claus
3302	103	10.2	Eligibility Evaluation Criteria - S.No. 7	7. The Bidder must have successfully supplied, installed and maintained (or under maintenance) SIEM Solution of minimum 20000 EPS / 0.86 TB per day in one PSU/ PSE/ Government Organizations / BFSI/Telecom provider in India in last 5 years	Request to change the clause condition and extend it to global and enterprise customer as well	Please refer addendum for revised clause.
3303	113	10.2	Eligibility Evaluation Criteria - S.No. 20	20. The proposed OEM solution should have been implemented in at least one BFSI is to be submitted for the following solutions: 1. SOAR 2. UEBA 3. Extended Detection & response (XDR) 4. Network Detection & response (NDR) 5. Threat Intelligence Platform	Request to modify the clause to allow credentials for implementation of similar/equivalent solutions from any OEM, rather than restricting the experience to the proposed OEM solution. The Bidder may have successfully implemented a similar solution using a different OEM in the past, which should be considered as valid experience demonstrating the Bidder's capability to implement and manage such solutions. Further, it is requested that credentials of either the Bidder or the proposed OEM be accepted. In case the Bidder does not have the requisite credentials, relevant credentials of the proposed OEM may be considered. Experience across BFSI/non-BFSI enterprise customers in India or globally may also kindly be accepted.	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3304	30	7.2.1 Solutions – Master Deployment Matrix	#8. Vulnerability assessment (VA) & vulnerability lifecycle management	Bank Location: Standalone at DC and Standalone at DR. Management Console: Deployed at both DC and DR	As per this RFP Technical Specification of VA & VLM,document #1788963129, #12 "The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and failover capabilities" where the 7.2.1 of suggests standalone deployment at DC, DR and console availablity at both DC and DR. These two partially contradict each other. We request you to kindly confirm if standalone VA & VM in DC and DR are expected to function independently. Maintaining two standalone environments with both consoles accessibility will lead to duplication of vulnerabilities, configuration efforts and it will cost upto 2X in terms of licensing. Though its not clear but we assume that you need one VM in DC and one in DR where primary one shares configuration backup on secondary and secondary can take over when the primary goes down, the primary VM solution should be able to scan both the DCs and vice-versa. If this understanding is correct, kindly update the clause as following - 'The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and active-cold standby failover capabilities where only one active console shall be accessible at a time'.	No Change, Please be guided by the RFP
3305	260	16.21.2 Volumetrics-Solution-wise Requirements	10 Vulnerability Assessment & Management (VA-VM) Minimum Numbers of IPs: 4000	10 Vulnerability Assessment & Management (VA-VM) Minimum Numbers of IPs: 4000	As per the RFP #1788963158, page 257 16.21.1 Current IT assets, P&SB has 2500 servers, 300 DB, 200 Apps, 12000 endpoints/desktops and 7200 routers and switches whereas the VA/VM IP coverage is mention as "Minimum" 4000. We seek your guidance and confirmation on the final count of assets/IPs you need coverage from day #1, given "minimum" count may lead to each bidder proposing seperate numbers and very likely excluding important assets from highly important VA & VM exercise. Without a defined and finite asset count, bidders cannot be compared on a like-for-like basis as the ones concerned about the VA/VM security posture of the infra will propose to cover more IPs/Assets while some may cover bare minimum and appear more competitive. We request you to kindly provide the final IP count required for VA/VM from day #1 considering the licenses are bound to assets and deleting the asset will delete all historic vulnerability and trends data, deleted asset will not cover alerts, ITSM integration and cannot be considered as part of VM exercise. As per the CERT'in recommendations (https://www.cert-in.org.in/PDF/guidelinesgovtentities.pdf) as well as industry best practices, entire ICT infrastructure should be part of the vulnerability management exercise and network device inclusion is absolute must given these are critical assets and in some zones exposed directly to internet.	No Change, Please be guided by the RFP
3306	38	On premises deployment of solutions	Storage Capacity & Sizing	• The Bidder shall provide detailed storage sizing based on expected data/log volumes, peak ingestion rate, retention period, indexing, enrichment, compression, replication, backup, archival and anticipated annual growth. Adequate capacity shall be provisioned for the complete contract period.	As per the RFP #1788963158, storage duration on the primary storage of the solution itself is mention for Cloud/SaaS/Hybrid to be 3 months, same is not clearly specified for VA & VM. Kindly confirm how long should the VA & VM solution retain the asset, vulnerability, logs, activities, historic trend etc. As per CERT-IN it must be 6 months. Kindly confirm if you wish the solution to retain this info on its own primary storage to be for 6 months or less.	Please refer addendum for revised clause
3307	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - VA-VM	VA-VM S.No. 9	Each scanning engine shall support web application security assessment together with traditional infrastructure vulnerability and configuration/compliance assessment. The solution shall identify vulnerabilities, missing patches, insecure configurations, and compliance deviations, and generate comprehensive reports containing risk severity, evidence of findings, affected assets, and remediation recommendations to support security governance, audit, and regulatory compliance.	While its possible to perform this via VA VM solution with additional WAS/DAST license, this will be a duplication of solution given you are already asking for seperate 'Application Security Testing Tool'. Hence, we request you to kindly move the 'Web application security assessment' from VA & VM requirements to DAST as this is a DAST requirement and may unnecessorily require to duplicate the licenses, solution and hardware.	No Change, Please be guided by the RFP
3308	Functional Compliance Sheet pp.48-51 (Appendix 1A)	Appendix 1A - VA-VM	VA-VM S.No. 36-52 and S.No. 61-77; S.No. 87 and S.No. 89	All technical compliances of VA-VM S.No. 36-52 and S.No. 61-77; S.No. 87 and S.No. 89	S.N 61-77 are likely duplicates of S.N 36 to 52 with minor changes. Request you to kindly review and confirm if this is intentional or typo. If not intentional, kindly remove duplicates to have the score calculated accordingly.	No Change, Please be guided by the RFP
3309	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 12	The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and failover capabilities.	VM solution is not an inline and always active solution.VM solutions across the industry do not have failovers similar to inline solutions such as firewalls. Hence, we request you to kindly consider the failover scenario as active - cold standby with documented backup-restore and a controlled switchover in place of automatic console failover. We request you to kindly update the clause as - The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and failover capabilities either automatically or using manual and controlled backup restore.	No Change, Please be guided by the RFP
3310	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 15	The proposed solution shall support integration with SIEM, SOAR, Threat Intelligence Platforms, NAC, and other security platforms through APIs or standard integration mechanisms.	Kindly share details (Vendor/Model/Version) of the SIEM, SOAR, TIP and NAC solution you would want to integrate with for us to identify the availablity of standard or API based integration and accordingly finalize the deployment efforts.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3311	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 16	The proposed solution shall integrate with Privileged Access Management (PAM) solutions for secure credential management during authenticated scans.	Kindly share details (Vendor/Model/Version) of the PAM solution you would want to integrate with for us to identify the availablity of integration and also identify the deployment efforts.	Bank is currently procuring PAM solution through separate RFP.
3312	Functional Compliance Sheet p.47 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 17	The proposed solution shall integrate with IT Service Management (ITSM) and ticketing platforms for automated vulnerability tracking and remediation workflows.	Kindly share details (Vendor/Model/Version) of the ITSM solution you would want to integrate with for us to identify the availablity of standard or API based integration and accordingly finalize the deployment efforts.	ITSM - Manage Engine
3313	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 29	The proposed solution shall support vulnerability assessment and compliance reporting aligned with PCI DSS requirements.	We request you to kindly confirm whether you only require to perform PCI DSS internal scanning and reporting on-premises or you also require the PCI- ASV attestation. If Attestation is required, kindly share the exact asset count for which the attestation is needed and how many attestations are to be submitted within 1 year.	No Change, Please be guided by the RFP
3314	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 42	The solution shall support vulnerability assessment of VMware ESXi, Hyper-V, Nutanix AHV, Kubernetes, OpenShift and container platforms.	We request you to kindly confirm whether you need the OS and platform vulnerability assessment of these container solutions or you need a comprehensive container security solution with the ability to identity vulnerabilities of images, registries and their components. If you need comprehensive container security assessment, we request you to kinly move this required to CNAPP solution as its usually part of cloud security solutions and not VM solution.	No Change, Please be guided by the RFP
3315	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 45	The solution shall integrate with enterprise CMDB, ITSM, SIEM, SOAR, PAM and NAC platforms through secure REST APIs.	Kindly share details (Vendor/Model/Version) of the required solutions you would want to integrate with for us to identify the deployment efforts.	Please refer addendum for the revised clause Details shall be shared with successful bidder
3316	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 47	The solution shall support Multi-Factor Authentication (MFA), LDAP, Active Directory, SAML 2.0 and OpenID Connect authentication.	We request you to kindly remove the OpenID and update the clause as following - The solution shall support Multi-Factor Authentication (MFA via SAML and/or LDAP), LDAP, Active Directory, SAML 2.0.	No Change, Please be guided by the RFP
3317	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 48	The solution shall support secure encrypted communication using TLS 1.3 and cryptographic modules compliant with FIPS 140-3 or equivalent internationally recognized standards.	We request you to kindly allow the FIPS 140-2 or equivilent solution transitioning to FIPS 140-3 to participate and update the clause as following - The solution shall support secure encrypted communication using TLS 1.3 and cryptographic modules compliant with FIPS 140-2 or FIPS 140-3 or equivalent internationally recognized standards.	Please refer addendum for revised clause
3318	Functional Compliance Sheet p.48 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 51	The solution shall identify internet-facing assets and continuously monitor externally exposed services.	We request you to kindly remove this clause as its an ASM(Attack Surface Management) requirements which is already asked separate service based solution of the RFP.	Please refer the addendum for revised clause
3319	Functional Compliance Sheet p.49 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 56	The solution shall support digitally signed and password-protected reports with configurable retention and archival.	We request you to kindly update the clause as following - The solution shall support password-protected reports with configurable retention and archival.	Please refer addendum for revised clause
3320	Functional Compliance Sheet p.49 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 60	The solution shall provide comprehensive REST APIs and webhook support for automation and integration with enterprise security platforms.	We request you to kindly update the clause as following - The solution shall provide comprehensive REST APIs or webhook support for automation and integration with enterprise security platforms.	Please refer addendum for revised clause
3321	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 87	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	We request you to kindly remove this clause from VM VM and move it to CTEM as this is a CTEM requirement, a solution that can be cloud/SaaS based. Given the data soveraginity and sensitivity of bank's vulnerabilities data, the platform is correctly requested to be on-prem which shall also be able to function without any internet connectivity. Hence, AI powering the on-prem application to achieve all the listed items is not viable. We request you to kindly remove this point and move it to CTEM.	Please refer the addendum for revised clause
3322	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 88	Unified, correlated findings intelligence. Every scanning engine — across web, API, network and host, cloud, containers, mobile, source code, device configuration and identity — reports into a single normalized findings model..	This is a CTEM requirement as VM solution won't perform VA of source code, identity etc. Kindly move this from VA VM to CTEM requirements.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3323	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 89	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	This is a duplicate of S.N. #87, kindly remove it.	Please refer the addendum for revised clause
3324	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 90	Mobile Application Security Testing: The proposed solution shall support static security analysis of Android and iOS mobile application packages, including APK/AAB and IPA formats, and shall provide security assessment mapped to recognized mobile application security standards and methodologies such as OWASP MASVS and MASTG.	This is not part of any VA/VM solution in industry and belongs to application security testing. We request you to kindly move this to 'Application Security Testing Tool'.	No Change, Please be guided by the RFP
3325	Functional Compliance Sheet p.50 (Appendix 1A)	Appendix 1A - Functional Compliance Sheet (Solutions) - Vulnerability Assessment & vulnerability lifecycle Management (VA-VM)	S.No. 91	White-Label Reporting and Approval Workflow: The proposed solution shall support customizable/white-label security assessment reports, including organization-specific branding and configurable report content. The solution shall support role-based maker-checker workflow for report generation, review, approval, and controlled release of finalized reports.	We request you to kindly update the clause as following - White-Label Reporting and Approval Workflow: The proposed solution shall support customizable/white-label security assessment reports, including organization-specific branding and configurable report content. The solution shall support role-based access for report generation, review of the finalized reports.	Please refer addendum for the revised clause White-Label Reporting and Approval Workflow: The proposed solution shall support customizable/white-label security assessment reports, including organization-specific branding and configurable report content. The solution shall support role-based or maker-checker workflow for report generation, review, approval of finalized reports.
3326	92	7.18.1 Compute Infrastructure	10. Non-production:	10. Non-production: a) The non-production environments should have the same software and hardware setup as deployed in production environments meeting all RFP requirements.	While this clause suggests the hardware and software setup of non-prod to be same, "16.21 Annexure 21: Sizing/Volumetrics, Data Retention and Current Infrastructure" suggests the VM based solution to have minimum 10% size. Kindly confirm if the 10% requirement of non-production infra is for only licenses whereas the hardware specs are to be identical to prod or both the licenses as well as hardware/software specs to be 10% of the production infra. Also kindly confirm if the non-production is to be setup only at DC or DC as well as DR.	Please refer addendum for the revised clause
3327	Functional Compliance Sheet pp.47-51 (Appendix 1A)	Appendix 1A - VA-VM	TOTAL MARKS row and S.No. 1 to 94	TOTAL MARKS - 850	While the VA-VM section contains 94 scoreable clauses, each carrying Maximum Marks of 10, which totals 940 marks, whereas the TOTAL MARKS row of the section states 850. We request you to kindly publish the corrected total and confirm the marks allocated per clause, so that bidders can compute the Respective Solution Compliance required by the Appendix 1A summary sheet consistently.	Please refer addendum for the revised clause
3328	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 19, 20, 43 and 44 (missing) and TOTAL MARKS row	CNAPP section is numbered from S.No. 1 to S.No. 60; however S.No. 19, 20, 43 and 44 do not appear in the sheet. TOTAL MARKS - 560.	The CNAPP section is numbered up to S.No. 60 but S.No. 19, 20, 43 and 44 are not present, leaving 56 scoreable clauses which, at 10 marks each, reconciles to the stated TOTAL MARKS of 560. We request you to kindly confirm whether these four clauses have been intentionally deleted or have been inadvertently omitted from the published sheet. If clauses exist against these serial numbers, kindly publish them along with the revised TOTAL MARKS; if they have been deleted, kindly re-issue the sheet with continuous numbering so that bidders' compliance responses and score computation remain traceable to the Bank's evaluation sheet.	Please refer addendum for the revised clause
3329	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 16	The solution shall support integration with relevant source-code repositories, development tools, build systems, CI/CD platforms and security workflows, either natively or through supported connectors/APIs.	A CNAPP integrates with source-code repositories and CI/CD platforms for Infrastructure-as-Code (IaC), container image and cloud-configuration assessment. It does not act as a source-code security testing tool, which is the function of the separately procured 'Application Security Testing Tool' in this RFP. We request you to kindly update the clause as following - "The solution shall support integration with relevant source-code repositories, development tools, build systems, CI/CD platforms and security workflows, either natively or through supported connectors/APIs, for the purpose of Infrastructure-as-Code, container image and cloud configuration assessment."	No Change, Please be guided by the RFP
3330	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 17 and S.No. 18	S.No. 17 - The solution shall identify security risks and known vulnerabilities associated with third-party, open-source and externally sourced software components and dependencies used by cloud-native applications. S.No. 18 - The solution shall provide visibility into application dependencies and software components and shall identify affected applications where a vulnerable component or dependency is detected.	Identification of third-party/open-source components and application dependencies is a Software Composition Analysis (SCA)/SBOM capability which belongs to the 'Application Security Testing Tool' scope already sought separately in this RFP, and requiring it again under CNAPP will lead to duplication of licences and cost without additional security benefit to the Bank. We request you to kindly either move these clauses to the Application Security Testing Tool requirements, or update them as following - "The solution shall identify known vulnerabilities in third-party and open-source software components and dependencies present within container images, registries and cloud workloads assessed by the platform, and shall identify the affected cloud-native applications/components."	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3331	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 24	The solution shall provide security visibility for cloud-native APIs and application interfaces, including risks related to exposure, authentication, authorization, access control and relevant configurations, where supported.	Discovery and security assessment of application APIs (including authentication/authorization testing of API endpoints) is the function of a dedicated API Security/API posture solution, and is not a native capability of CNAPP platforms. CNAPP platforms provide visibility of cloud-native API gateway and managed API service configurations and their exposure. We request you to kindly update the clause as following - "The solution shall provide security visibility for cloud-provider API gateway/managed API services and application interfaces discovered from the cloud control plane, including risks related to public exposure, authentication/authorization configuration and access control settings, where supported by the respective cloud platform."	No Change, Please be guided by the RFP
3332	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 26	The solution shall provide visibility into application access to sensitive or critical data and identify security risks arising from inappropriate application access, exposure or relationships, where supported.	As worded, this clause can be read as requiring full Data Security Posture Management (DSPM) with data discovery and classification of the Bank's data stores, which is a separately licensable product category and is not part of a baseline CNAPP. We request you to kindly confirm whether DSPM (data discovery and classification) is intended to be in scope of the CNAPP. If it is not intended, we request you to kindly update the clause as following - "The solution shall provide visibility into application and identity access paths to cloud data stores and shall identify security risks arising from public exposure, excessive access or inappropriate relationships to such data stores, where supported by the respective cloud platform." If DSPM is intended, kindly publish the applicable volumetrics (number/size of data stores) so that bidders can size and price the module consistently.	No Change, Please be guided by the RFP
3333	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 27	The solution shall identify vulnerable application components that are reachable, exposed or potentially exploitable within the application's dependency or relationship graph, where such analysis is supported.	Code-level 'reachability' analysis of a vulnerable function within an application's dependency graph is an SCA/ASPM capability delivered by application security testing tools. CNAPP platforms determine exposure and exploitability from cloud context - internet exposure, network path, identity privilege and attack-path relationships. We request you to kindly update the clause as following - "The solution shall identify vulnerable application components that are internet-exposed, network-reachable or potentially exploitable based on cloud exposure, network path, identity privilege and attack-path relationship analysis, where such analysis is supported by the proposed solution."	No Change, Please be guided by the RFP
3334	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 32	The solution shall provide guided, semi-automated and/or automated remediation capabilities for supported application-security findings.	Fully automated remediation executed directly by a security platform on a production banking cloud environment is generally not permitted under change-management controls, and CNAPP platforms deliver remediation as guided steps and auto-generated remediation artefacts (e.g., IaC fix code/pull requests, CLI commands, policy snippets) which are then applied by the Bank/implementation partner through the Bank's change process. We request you to kindly update the clause as following - "The solution shall provide guided remediation and automatically generated remediation artefacts (such as IaC remediation code, pull requests, CLI commands or policy snippets) for supported application-security findings, which may be applied through the Bank's approved change-management process or through integration with the Bank's SOAR/ITSM platform."	No Change, Please be guided by the RFP
3335	Functional Compliance Sheet (Appendix 1A) - CNAPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud-Native Application Protection Platform (CNAPP)	CNAPP S.No. 59	The solution shall support high availability and service continuity appropriate to the proposed deployment architecture and shall provide mechanisms for recovery of relevant configurations, policies and security information.	Where the CNAPP is delivered as OEM-managed SaaS, high availability, redundancy, backup and disaster recovery are provided by the OEM within the platform and are governed by the OEM's published availability SLA; the Bank cannot be provided Bank-operated HA/DR or restore mechanisms for a SaaS platform. We request you to kindly update the clause as following - "For SaaS-delivered solutions, the OEM shall provide high availability, redundancy and disaster recovery within the platform in line with its published availability SLA, and shall provide mechanisms for export/retrieval of relevant configurations, policies and security information. For on-premises components, if any, the solution shall support HA and documented backup-restore."	Please refer to the addendum: The solution shall support service continuity appropriate to the proposed deployment architecture and shall provide mechanisms for recovery of relevant configurations, policies and security information.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3336	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP - Section scope (S.No. 1 to 50, principally S.No. 1, 6, 7, 8 to 41)	The proposed Cloud Workload Protection Platform (CWPP) shall provide centralized capabilities for protecting, monitoring, detecting, investigating and responding to security threats affecting cloud workloads during runtime. (S.No. 1) and the runtime detection, prevention, response, forensics and threat-hunting clauses at S.No. 6 to 41.	The CWPP section as drafted is predominantly a runtime endpoint/server threat prevention, detection and response (EDR/XDR-class) specification - in-guest malware and ransomware prevention, exploit prevention, host IDS/IPS, file integrity monitoring, process and command-line telemetry, containment actions such as process termination, file quarantine and workload isolation, forensic timelines, process trees and threat hunting. These are delivered by an EDR/XDR agent platform, whereas the CNAPP/CWPP category referenced elsewhere in this RFP delivers agentless workload vulnerability, malware, misconfiguration, identity, secrets and exposure assessment with attack-path context. Given the Bank is separately procuring EDR/XDR and SOC/SIEM capabilities under this very RFP, we request you to kindly clarify and confirm any one of the following, so that bidders are not compelled to bid a second endpoint agent on the same servers: 1. That runtime prevention, containment and forensics requirements of the CWPP section may be met through the Bank's in-scope EDR/XDR platform, with the CWPP providing agentless workload exposure assessment, posture and attack-path context integrated with it; or 2. That the CWPP section may be responded to on a multi-OEM/consortium basis with clear identification of the product meeting each clause (consistent with S.No. 50 of this section); or 3. That the runtime prevention/response clauses be moved	No Change, Please be guided by the RFP
3337	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 2 and S.No. 3	S.No. 2 - The solution shall support protection of workloads deployed across physical, virtual, private-cloud, public-cloud and hybrid-cloud environments, as applicable. S.No. 3 - The solution shall support major public-cloud environments including AWS, Microsoft Azure and Google Cloud Platform, as applicable.	CWPP licensing and sizing depend entirely on the workload inventory in scope, and the clause extends coverage to physical and private-cloud workloads in addition to public cloud. We request you to kindly publish, for the CWPP scope, the workload volumetrics for day #1 and for the contract period - number of physical servers, virtual machines, public-cloud instances (per CSP), container hosts/nodes, Kubernetes clusters and serverless functions - along with the CSP accounts/subscriptions/projects in scope. Kindly also confirm which of these environments are mandatory on day #1, since 'as applicable' may lead each bidder to price a different scope and render the commercial bids non-comparable.	No Change, Please be guided by the RFP
3338	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 8, S.No. 21 and S.No. 22	S.No. 8 - The solution shall detect and prevent, where supported, malware, ransomware, trojans, rootkits and other malicious software or activities affecting protected workloads. S.No. 21 - The solution shall provide protection against ransomware and destructive activities, including detection of abnormal file encryption or mass file modification behavior. S.No. 22 - The solution shall provide exploit detection and/or prevention capabilities for supported workload operating systems and applications.	In-guest prevention of malware, ransomware, trojans and rootkits, behavioural detection of mass file-encryption, and memory/exploit prevention require a kernel-level endpoint prevention engine (EDR/EPP) and are not functions of an agentless cloud workload protection platform, which performs malware and vulnerability detection through workload snapshot/disk analysis without in-line blocking. We request you to kindly move these clauses to the EDR/XDR section of the RFP, or update them as following - "The solution shall detect malware, ransomware, trojans, rootkits, malicious files and destructive activity affecting protected workloads through agentless and/or agent-based assessment, and shall support prevention/blocking natively or through integration with the Bank's EDR/XDR platform."	S.No. 8- No Change, Please be guided by the RFP S.No. 21- No Change, Please be guided by the RFP S.No. 22- No Change, Please be guided by the RFP
3339	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 9 to S.No. 14	S.No. 9 to 14 - monitoring of process execution and process behaviour; detection of suspicious process chains and abnormal parent-child relationships; monitoring of command-line execution, scripts and interpreters; detection of Living-off-the-Land techniques; behavioural/heuristic analysis of anomalous activity; and detection of privilege escalation, persistence, lateral movement and credential misuse.	These clauses describe in-guest runtime behavioural telemetry (process, command-line, script and parent-child process monitoring) which is collected by an EDR/XDR sensor and analysed in the SOC/SIEM. A CWPP that assesses workload exposure agentlessly does not generate kernel-level process telemetry. We request you to kindly move these clauses to the EDR/XDR section, or update them as following - "The solution shall provide the specified runtime behavioural detection capabilities natively or through correlation of telemetry from the Bank's EDR/XDR and SIEM platforms, and shall enrich such detections with workload vulnerability, identity, configuration and exposure context." Kindly also confirm that a capability delivered through such integration will not be treated as non-compliant, consistent with the principle already accepted at CNAPP S.No. 53 of this Appendix.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3340	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 15, S.No. 16 and S.No. 17	S.No. 15 - The solution shall monitor relevant network communications involving protected workloads and identify suspicious or unauthorized communication patterns. S.No. 16 - The solution shall identify communication with known or suspected malicious infrastructure, including malicious IP addresses, domains, URLs, command-and-control infrastructure or equivalent threat indicators, where applicable. S.No. 17 - The solution shall provide host/workload-based intrusion detection and/or prevention capabilities for supported operating systems and workloads.	Host-based intrusion detection/prevention and in-line inspection of workload network traffic for command-and-control communication are functions of HIDS/HIPS agents, NDR and NGFW/IPS controls, all of which are separately in scope in this RFP. A CWPP provides network exposure and reachability analysis from cloud configuration (security groups, NACLs, routes, load balancers, public exposure) rather than packet-level inspection. We request you to kindly move these clauses to the EDR/XDR, NDR or NGFW sections as appropriate, or update them as following - "The solution shall identify workload network exposure, reachable paths and unauthorized/high-risk communication paths from cloud network configuration and available flow logs, and shall support identification of communication with known malicious infrastructure natively or through integration with the Bank's EDR/XDR, NDR, NGFW and SIEM platforms."	S.No. 15- No Change, Please be guided by the RFP S.No. 16- No Change, Please be guided by the RFP S.No. 17- No Change, Please be guided by the RFP
3341	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 18 and S.No. 19	S.No. 18 - The solution shall monitor critical files, directories, system objects and configuration elements for unauthorized modification, creation or deletion, where supported. S.No. 19 - The solution shall provide file integrity monitoring for designated critical files, directories and system objects.	File Integrity Monitoring (FIM) requires a resident agent performing real-time file-system event monitoring on the workload and is a standard EDR/host-integrity capability. It is not delivered by an agentless cloud workload protection platform. We request you to kindly move these clauses to the EDR/XDR section, or update them as following - "File integrity monitoring for designated critical files, directories and system objects shall be provided natively or through integration with the Bank's EDR/XDR or host-integrity solution, with the resulting events available for correlation and reporting."	No Change, Please be guided by the RFP
3342	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 20 and S.No. 24	S.No. 20 - The solution shall detect suspicious creation or modification of system accounts, services, scheduled tasks and other persistence mechanisms, where applicable. S.No. 24 - The solution shall support detection and/or prevention of web-shell and other unauthorized application-level persistence mechanisms, where applicable.	Real-time detection of persistence mechanisms and prevention of web-shell execution are runtime endpoint and web application protection (EDR/WAF) functions. A CWPP can identify such artefacts through periodic workload assessment but cannot prevent their execution. We request you to kindly move these clauses to the EDR/XDR and WAF sections respectively, or update them as following - "The solution shall identify unauthorized accounts, services, scheduled tasks, web-shells and other persistence artefacts present on assessed workloads, and shall support real-time detection/prevention natively or through integration with the Bank's EDR/XDR and WAF platforms."	No Change, Please be guided by the RFP
3343	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 23	The solution shall support virtual patching or equivalent compensating protection mechanisms, where applicable, for vulnerabilities for which immediate patching is not feasible.	Virtual patching is enforced by in-line controls - host IPS agents, NGFW/IPS and WAF - all of which are separately procured under this RFP. A workload protection/exposure platform identifies the vulnerability and recommends the compensating control; it does not itself enforce a virtual patch. We request you to kindly remove this clause from the CWPP section as it is already covered by the Bank's NGFW/IPS and WAF requirements, or update it as following - "For vulnerabilities where immediate patching is not feasible, the solution shall identify the exposure, provide risk context and recommend applicable compensating controls, which may be enforced through the Bank's in-line security controls (host IPS, NGFW/IPS, WAF) through supported integration."	No Change, Please be guided by the RFP
3344	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 25, 26, 27 and 28	S.No. 25 - runtime security monitoring and threat detection for containerized workloads; S.No. 26 - runtime protection for Kubernetes workloads including pods, containers and workload processes; S.No. 27 - detection of suspicious behaviour involving containers, pods, workload processes and workload-to-workload communications; S.No. 28 - security monitoring for serverless workloads/functions.	Container and Kubernetes runtime protection requires a privileged runtime sensor (e.g., eBPF/DaemonSet-based) on every node, which materially differs from the container and Kubernetes security posture, image/registry scanning, admission control and Kubernetes misconfiguration and RBAC assessment delivered by a CNAPP/CWPP. We request you to kindly clarify whether the Bank requires (a) container/Kubernetes runtime sensor-based prevention or (b) container and Kubernetes security posture with image, registry, IaC, admission-control and RBAC assessment plus runtime detection through the Bank's EDR/XDR on the worker nodes. We request you to kindly permit option (b) and update the clauses to allow the capability to be delivered through posture assessment, admission control and integration with the Bank's EDR/XDR and SIEM, failing which the clause is restrictive to a small subset of OEMs. Kindly also publish the number of Kubernetes clusters, nodes and serverless functions in scope for sizing.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3345	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 29 and S.No. 30	S.No. 29 - The solution shall support agent-based and/or agentless protection mechanisms, as applicable to different workload types and supported environments. S.No. 30 - Where an agent is required, the solution shall provide mechanisms for secure deployment, centralized management, health monitoring and controlled upgrade of the workload protection agent.	We note and appreciate that S.No. 29 permits agentless mechanisms. However, several other clauses in this section (S.No. 8 to 41) are achievable only through an in-guest agent, which contradicts the option provided in S.No. 29. We request you to kindly confirm that an agentless-first architecture, supplemented where required by the Bank's EDR/XDR agent already deployed on the workloads, will be accepted as compliant against this section, and that S.No. 30 shall apply only where the bidder proposes its own agent. Kindly also confirm that no additional agent is mandated on workloads that already carry the Bank's EDR/XDR agent, in view of performance and change-management impact on production banking workloads.	No Change, Please be guided by the RFP
3346	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 32 and S.No. 33	S.No. 32 - The solution shall support configurable response actions for detected threats, including alerting, blocking, process termination, file quarantine, workload isolation or other equivalent containment actions, as applicable. S.No. 33 - The solution shall provide workload isolation or containment capabilities to limit the impact or spread of a confirmed or suspected compromise, where supported.	Process termination, file quarantine and host/network isolation are kernel-level containment actions performed by an EDR/XDR agent. An agentless workload protection platform performs cloud-control-plane actions (such as snapshotting, tagging, security-group/identity restriction) and orchestrates containment through the Bank's EDR/XDR and SOAR. We request you to kindly move these clauses to the EDR/XDR section, or update them as following - "The solution shall support configurable response actions for detected threats, including alerting, notification, cloud-control-plane containment actions (such as network/identity restriction, snapshot and tagging) natively, and process termination, file quarantine and workload isolation through integration with the Bank's EDR/XDR and SOAR platforms."	S.No. 32 - No Change, Please be guided by the RFP S.No. 33 - No Change, Please be guided by the RFP
3347	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 34, 35, 36 and 37	S.No. 34 - security investigation using process, file, network, user, workload and event-level information; S.No. 35 - historical workload activity and security-event information sufficient for investigation and forensic analysis; S.No. 36 - process-tree or equivalent process-relationship visualization; S.No. 37 - workload-level threat hunting using available security telemetry and configurable search criteria.	Retention of process/file/network event-level telemetry, process-tree reconstruction and telemetry-based threat hunting are EDR/XDR and SIEM functions and require an in-guest sensor. Additionally, these clauses do not specify a retention period, which makes consistent sizing and pricing impossible. We request you to kindly (a) move these clauses to the EDR/XDR and SIEM sections or permit compliance through integration with the Bank's EDR/XDR and SIEM platforms, and (b) if retained under CWPP, publish the mandated telemetry retention period (hot/warm/archive) and the expected daily event volume per workload, so that all bidders size storage and licences on a common basis.	No Change, Please be guided by the RFP
3348	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 38 and S.No. 39	S.No. 38 - The solution shall support identification and searching of Indicators of Compromise (IoCs), including supported hashes, IP addresses, domains, URLs and equivalent indicators. S.No. 39 - The solution shall support integration with external threat-intelligence sources to enhance workload threat detection and investigation.	Retrospective and real-time IoC sweeps across workloads are performed on EDR/XDR telemetry or in the SIEM, where the Bank's threat-intelligence platform feeds are already consolidated under this RFP. We request you to kindly update the clauses as following - "The solution shall support identification and searching of Indicators of Compromise (hashes, IP addresses, domains, URLs and equivalent indicators) against available workload assessment data natively, and across workload runtime telemetry through integration with the Bank's EDR/XDR, SIEM and threat-intelligence platforms. The solution shall support ingestion of external threat-intelligence to enrich and prioritise workload findings."	No Change, Please be guided by the RFP
3349	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 47 and S.No. 48	S.No. 47 - The solution shall support high availability and service continuity appropriate to the proposed deployment architecture and shall provide mechanisms for recovery of relevant configurations and security policies. S.No. 48 - The solution shall provide mechanisms to identify the protection health/status of onboarded workloads, including agent, connector or communication health where applicable.	For OEM-managed SaaS delivery, high availability, redundancy and disaster recovery are provided within the OEM platform under its published availability SLA and cannot be operated or restored by the Bank. We request you to kindly update S.No. 47 as following - "For SaaS-delivered solutions, the OEM shall provide high availability, redundancy and disaster recovery within the platform in line with its published availability SLA and shall provide mechanisms for export/retrieval of relevant configurations and security policies. For on-premises components, if any, the solution shall support HA and documented backup-restore." For S.No. 48, we request confirmation that reporting of connector/cloud-account onboarding and assessment health (and agent health only where an agent is proposed) shall be treated as compliant.	Please refer addendum for revised clause S.No. 47 - The solution shall support service continuity appropriate to the proposed deployment architecture and shall provide mechanisms for recovery of relevant configurations and security policies. Clarification S.No. 48 - Bidder to propose the aproach ensuring the compliance with the sought requirement. Reporting of connector/cloud-account onboarding and assessment health shall also be considered compliant. Agent health reporting shall apply only where an agent is proposed/deployed.
3350	Functional Compliance Sheet (Appendix 1A) - CWPP	Appendix 1A - Functional Compliance Sheet (Solutions) - Cloud Workload Protection Platform (CWPP)	CWPP S.No. 49	The solution shall support consumption and correlation of relevant vulnerability, SBOM, CBOM and threat-intelligence information from the Bank's separately procured security solutions through APIs, supported integrations or equivalent mechanisms, where technically supported.	Consumption of Cryptographic Bill of Materials (CBOM) is an emerging requirement with no single established interchange standard, and correlation is only feasible if the source system and format are known. We request you to kindly confirm (a) the source solutions and the exact formats/standards in which SBOM and CBOM will be provided by the Bank (e.g., CycloneDX, SPDX and version), and (b) that where a standard format/API is not made available by the source solution, non-availability of such correlation shall not be treated as non-compliance, consistent with the qualifier 'where technically supported' in the clause.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3351	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM - Section scope (S.No. 1 to 69 and TOTAL MARKS 690)	Continuous Threat Exposure Management (CTEM) - all functional specifications, S.No. 1 to 69, TOTAL MARKS 690.	A significant proportion of the CTEM section (illustratively S.No. 1, 2, 5, 7 to 13, 18 to 23, 35, 55, 56, 57 and 67) specifies Cyber Threat Intelligence (CTI) and Digital Risk Protection (DRP) service deliverables - multilingual dark-web collection and translation, analyst-authored periodic and ad-hoc research reports, VIP investigation reports, threat-actor dossiers and engagement with threat actors, compromised-credential and payment-card monitoring, takedown/reporting to external authorities, named analyst and incident-response services. These are analyst-delivered managed services and are distinct from a Continuous Threat Exposure Management platform, which (per the recognised CTEM framework) delivers scoping, discovery, prioritisation, validation and mobilisation of exposures across the attack surface. As currently drafted, the section can be fully met only by DRP/CTI service providers and is restrictive to exposure-management platform OEMs, even though the Bank has separately (at VA-VM S.No. 87 and 88) contemplated CTEM as the platform that consolidates and prioritises findings across scanning engines. We therefore request you to kindly split this section into (a) 'CTEM / Exposure Management Platform' and (b) 'Cyber Threat Intelligence and Digital Risk Protection Services', with separate functional specifications, separate marks and separate	No Change, Please be guided by the RFP
3352	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 1, S.No. 2 and S.No. 7	S.No. 1 - The solution should collect intelligence from multiple languages and relevant regional sources, with support for multilingual threat intelligence processing and analysis. S.No. 2 - The solution should support translation or interpretation of collected intelligence into English. S.No. 7 - Each intelligence item should include metadata such as date, author, source, and pre-classification of raw data.	Multilingual collection from closed/regional sources, machine translation of collected raw intelligence, and 'author'-level metadata with pre-classification of raw data are characteristics of a dark-web/DRP collection platform and are not features of a CTEM/exposure management platform. We request you to kindly move these clauses to the proposed Cyber Threat Intelligence/DRP service scope. If they are retained under CTEM, we request you to kindly update them as following - "The solution shall provide vulnerability, exploit and exposure intelligence in English, with source, publication date and classification metadata, and shall support ingestion of multilingual/regional intelligence from bank-approved third-party sources through supported integration mechanisms."	Please refer the addendum for revised clause
3353	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 8 and S.No. 53	S.No. 8 - The solution should allow messaging and collaboration within the context of a specific intelligence item. S.No. 53 - Each alert should include a discussion board for eligible users to collaborate within the alert context.	An in-product messaging/discussion board is a vendor-specific user-interface feature, and for a bank, collaboration and audit trails on security findings are better retained in the Bank's ITSM/SOAR system of record rather than in a third-party SaaS console. We request you to kindly update the clauses as following - "The solution shall support collaboration on a specific exposure, alert or intelligence item through comments/annotations, assignment and status tracking within the platform and/or through bidirectional integration with the Bank's ITSM/SOAR/ticketing platform."	No Change, Please be guided by the RFP
3354	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 9	The solution shall provide access to proprietary, internally generated, licensed or equivalent high-quality threat intelligence sources capable of providing actionable intelligence relevant to the Bank's environment.	We request confirmation of the nature of intelligence expected. Exposure-management OEMs provide proprietary research-generated vulnerability, exploit and exposure intelligence (including exploit availability, exploitation-in-the-wild, ransomware association and predictive exploitability), whereas dark-web/actor intelligence is sourced by DRP providers. We request you to kindly update the clause as following - "The solution shall provide access to the OEM's proprietary/internally generated and/or licensed intelligence covering vulnerabilities, exploits, exploitation activity and exposures relevant to the Bank's environment, and shall support ingestion of additional bank-approved third-party intelligence sources."	No Change, Please be guided by the RFP
3355	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 10	Analysts should perform threat hunting activities to find findings outside of the platform.	This clause requires a human analyst-delivered managed service and is not a functional specification of a solution. Scoring it within a functional compliance sheet at 10 marks does not permit objective evaluation. We request you to kindly move this clause to the managed services/MSSP or CTI service scope of the RFP with defined service levels (number of analyst hours, hunting frequency, deliverable and reporting format) and a separate commercial line item, so that bidders can price it objectively. If it is retained, kindly define the expected analyst effort and deliverables.	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3356	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 11	The solution/service should generate investigation reports for designated VIPs or other high-risk identities/assets, providing an overview of identified digital exposure and associated risk.	VIP/executive digital exposure investigation is a Digital Risk Protection service deliverable involving collection of personal digital footprint data, and carries data-protection considerations under the DPDP Act for the named individuals. We request you to kindly move this clause to the Cyber Threat Intelligence/DRP service scope. If retained, kindly confirm the number of designated VIPs/high-risk identities, the frequency of such reports and the consent/lawful-basis framework the Bank will provide for processing their personal data, so that bidders can price and lawfully deliver the service.	No Change, Please be guided by the RFP
3357	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 5, S.No. 12 and S.No. 13	S.No. 5 - automated and/or AI-assisted generation of tailored intelligence reports based on customer requirements. S.No. 12 - general and industry-related cyber intelligence reports on threat landscape trends, at least twice a month. S.No. 13 - the solution should be able to commission ad-hoc research reports on demand.	Periodic (twice monthly) industry threat-landscape reports and ad-hoc commissioned research reports are analyst-authored service deliverables, and 'on demand' without a defined ceiling is commercially open-ended. We request you to kindly move these clauses to the Cyber Threat Intelligence service scope with defined deliverables, and kindly confirm (a) the maximum number of ad-hoc research reports that may be commissioned per annum, (b) the expected turnaround time, and (c) whether these are to be priced within the platform subscription or as a separate service line item.	a. Periodic industry threat-landscape reports - At least a month b. Ad-hoc commissioned research reports: The requirement shall shall relate to threats, exposures, vulnerabilities and risk areas relevant to the Bank c. Bidder to ensure that all requite cost is factored and the requirement is complied at not additional to the bank Please refer addendum for revised clause
3358	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 18	The solution should provide comprehensive threat actor attribution including known identities, motivations, historical activity, TTPs, associated infrastructure, and MITRE ATT&CK mapping.	Threat-actor attribution dossiers covering actor identities, motivations and associated infrastructure are CTI/DRP deliverables. Exposure-management platforms provide threat-actor and campaign context mapped to MITRE ATT&CK for the vulnerabilities and exposures identified in the Bank's environment. We request you to kindly move this clause to the Cyber Threat Intelligence service scope, or update it as following - "The solution shall provide threat context for identified exposures, including associated threat actors/campaigns, observed exploitation activity, TTPs and MITRE ATT&CK mapping, where such intelligence is available, and shall support enrichment from bank-approved third-party threat-intelligence sources."	Please refer addendum for revised clause
3359	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 19	The solution should detect compromised credentials for employees and VIPs, exposed payment card information, and aggregate data from known breach databases in real time	Detection of compromised credentials and exposed payment-card data through aggregation of breach and dark-web databases is a Digital Risk Protection capability and requires the provider to collect, store and process the Bank's employees' and customers' personal and card data, with attendant DPDP Act and PCI DSS implications. We request you to kindly move this clause to the Cyber Threat Intelligence/DRP service scope of the RFP. If retained under CTEM, kindly confirm the employee/identity count and card-BIN ranges to be monitored, and the data-processing and retention framework the Bank will mandate for such personal and cardholder data.	Please refer addendum for revised clause
3360	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 21	The solution should support threat actor interaction via vendor analysts (e.g., engaging via dark web avatars) to gather additional intelligence	Engagement with threat actors through covert dark-web personas is offered by a very small number of DRP providers, cannot be objectively evidenced or evaluated in a technical compliance sheet, and exposes a regulated bank to legal, reputational and regulatory risk arising from interaction with criminal actors on its behalf. We request you to kindly remove this clause from the CTEM functional specifications, as it is restrictive to a limited set of vendors and is not required to achieve continuous threat exposure management outcomes. If the Bank wishes to retain such capability, we request it be moved to an optional service line item, excluded from the technical scoring.	Please refer addendum for the revised clause Clause Stands deleted
3361	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 23	The solution should support reporting of confirmed malicious or phishing assets to relevant external platforms and authorities, where such reporting is supported and authorized.	Reporting and takedown of malicious/phishing domains and assets with registrars, hosting providers, app stores and authorities is an anti-phishing/brand-protection service, delivered under authorisation letters from the brand owner. We request you to kindly move this clause to the anti-phishing/brand protection service scope. If retained, kindly confirm the expected number of takedown/reporting requests per annum and the applicable turnaround SLA, and confirm that the Bank will provide the requisite authorisation to act on its behalf, so that bidders can price the service.	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3362	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 20, 22, 45 and 47	S.No. 20 - IoC enrichment allowing submission of IPs, domains and hashes to receive contextual threat intelligence and threat actor attribution; S.No. 22 - scanning and reputation analysis of submitted IP addresses; S.No. 45 - manual IoC management operations; S.No. 47 - cross-platform IoC enforcement across the security stack.	IoC submission, enrichment, lifecycle management and - in particular - enforcement of IoCs across the security stack are functions of a Threat Intelligence Platform (TIP) and SOAR, both of which are in scope of this RFP. Enforcement (pushing blocklists to NGFW, proxy, DNS, EDR and email gateways) is performed by those controls under the Bank's change-management process, not by an exposure-management platform. We request you to kindly move S.No. 45 and S.No. 47 to the TIP/SOAR scope, and update S.No. 20 and S.No. 22 as following - "The solution shall support enrichment of submitted indicators (IP addresses, domains, hashes) with available contextual intelligence and reputation information natively and/or through integration with the Bank's threat-intelligence platform, and shall support publishing of validated indicators to the Bank's security controls through the Bank's SOAR/TIP."	Please refer addendum for the revised clause
3363	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 24	The solution should provide pre-built bidirectional integrations with SIEM, SOAR, ticketing (Manage Engine), and threat intelligence platforms	Availability of a 'pre-built' connector is vendor-specific, whereas equivalent bidirectional integration is routinely achieved through documented REST APIs and webhooks with the same functional outcome. We request you to kindly share the Vendor/Model/Version of the SIEM, SOAR, ManageEngine ticketing product and threat-intelligence platform to be integrated, and update the clause as following - "The solution shall provide bidirectional integration with the Bank's SIEM, SOAR, ticketing (ManageEngine) and threat-intelligence platforms through pre-built connectors, documented REST APIs, webhooks or equivalent mechanisms."	Please refer addendum for the revised clause
3364	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 30 and S.No. 33	S.No. 30 - The solution shall provide automated validation of identified exposures, where technically applicable and authorized by the Bank, using controlled, non-destructive testing or equivalent validation mechanisms to determine whether the identified exposure is genuinely exploitable or materially exposed. S.No. 33 - The solution should validate that a vulnerability is actually exploitable or otherwise materially exposed (active exposure validation).	Active, automated exploitation-based validation of findings is the function of Breach and Attack Simulation (BAS) or automated penetration-testing tooling - which the Bank itself references at S.No. 41 of this section as a separate external source to be integrated. Exposure-management platforms establish material exposure and exploitability through evidence-based validation: authenticated/unauthenticated verification of the finding, reachability and internet-exposure analysis, attack-path analysis, exploit availability and exploitation-in-the-wild intelligence. We request you to kindly update the clauses as following - "The solution shall validate whether an identified exposure is genuinely exploitable or materially exposed using evidence-based validation - including verification of the finding, internet exposure and network reachability analysis, attack-path analysis, exploit availability and observed exploitation intelligence - and shall support ingestion of validation results from the Bank's BAS/penetration-testing tools through supported integration." Kindly also confirm that active exploitation testing against the Bank's production environment is not mandated as a day #1 platform capability.	Please refer addendum for the revised clause
3365	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 35	The solution should detect malicious files, reconnaissance activity, automated attack tools, and target lists	Detection of reconnaissance activity, automated attack tooling and 'target lists' naming the Bank requires deception/honeypot sensors, network detection telemetry or dark-web collection, none of which are capabilities of a CTEM/exposure management platform. We request you to kindly remove this clause from the CTEM section (reconnaissance and attack-tool detection being already addressed by the Bank's NDR, WAF, NGFW and SOC/SIEM scope), or move it to the Cyber Threat Intelligence/DRP service scope.	Please refer addendum for revised clause
3366	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 41	The solution should support external vulnerability source integrations such as VA/VM scanners, ASM, XDR, BAS, Dark Web Monitoring, and MDM/UEM	Integration is feasible only where the source product, version and API are known, and Dark Web Monitoring and BAS are separate product categories which the Bank may or may not have licensed. We request you to kindly (a) share the Vendor/Model/Version of each source solution to be integrated (VA/VM, ASM, XDR, BAS, Dark Web Monitoring, MDM/UEM), (b) confirm which of these the Bank already owns and which are expected to be supplied by the bidder, and (c) confirm that non-availability of integration with a product the Bank has not licensed, or which does not expose a supported API, shall not be treated as non-compliance.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3367	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 42 and S.No. 43	S.No. 42 - The solution should use machine learning to evaluate the business impact of each remediation action and prioritize high-priority exposures. S.No. 43 - The ML model should continuously study the environment including asset relationships, topology, and security controls to detect false positives and identify root causes.	These clauses mandate a specific implementation mechanism ('machine learning', 'the ML model') and a specific analytic behaviour rather than the security outcome, which is restrictive to a particular OEM's product design. The Bank has adopted a technology-neutral formulation elsewhere in this very section (S.No. 34 - 'using AI/ML or equivalent analytic'). We request you to kindly update the clauses as following, consistent with S.No. 34 - "The solution shall prioritise exposures using AI/ML or equivalent analytics based on asset criticality and business context, exploitability, exposure, asset relationships/topology and the effect of existing security controls, and shall support identification of false positives and of common root causes to enable efficient remediation."	No Change, Please be guided by the RFP
3368	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 38 read with S.No. 41 and S.No. 48	S.No. 38 - The solution should be deployed agentlessly, without requiring sensors or agents on endpoints, servers, or network appliances. S.No. 41 - external vulnerability source integrations such as VA/VM scanners, ASM, XDR, BAS, Dark Web Monitoring, and MDM/UEM. S.No. 48 - The solution should assess and harden network, endpoint, and operating system security controls.	S.No. 38 mandates a fully agentless and sensor-less deployment, while S.No. 48 requires assessment and hardening of endpoint and operating-system security controls - which requires either a credentialed/authenticated scan, an agent, or ingestion from the agent-based VA/VM, XDR and MDM/UEM platforms referenced in S.No. 41. These clauses partially contradict each other. We request you to kindly confirm that the CTEM platform itself may remain agentless and derive endpoint/OS control assessment through integration with the Bank's VA/VM, XDR and MDM/UEM platforms and credentialed configuration audit performed by those tools, and kindly update S.No. 48 as following - "The solution shall consolidate and report on the configuration/hardening posture of network, endpoint and operating system security controls, natively and/or by ingesting configuration and compliance assessment results from the Bank's VA/VM, XDR, MDM/UEM and related platforms."	Please refer addendum for the revised clause
3369	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 49 and S.No. 50	S.No. 49 - The solution should provide a private exposure map of the organization's attack surface. S.No. 50 - The solution should support custom protections tailored to the organization's environment.	The terms 'private exposure map' and 'custom protections' are vendor-specific product terminology and are not objectively evaluable; 'protections' further implies enforcement, which a CTEM platform does not perform. We request you to kindly update the clauses as following - S.No. 49 - "The solution shall provide a consolidated, access-controlled map/inventory of the organisation's internal and internet-facing attack surface, including assets, relationships, exposures and attack paths." S.No. 50 - "The solution shall support custom policies, custom detection/assessment rules, custom risk scoring and custom tagging tailored to the organisation's environment."	S.No 49.: Please refer addendum for revised clause Clarification: S.No 50: " & M500
3370	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 51, 59, 60, 62 and 63	S.No. 51 - apply virtual patching/compensating controls/exposure mitigation mechanism to the firewall and other security systems through integration with relevant security controls; S.No. 59 - API-based remediation, notification or workflow integration with relevant security controls; S.No. 60 - automated remediation workflows; S.No. 62 - leverage compensating controls and layered defense strategies; S.No. 63 - collaboration tools and ITSM integration for remediation workflows.	These clauses require the CTEM platform to execute configuration changes directly on the Bank's production security controls (firewall, WAF, IPS, EDR). In a regulated banking environment such changes must pass through the Bank's change-management and maker-checker controls, and the accountable system of record for orchestration is the Bank's SOAR/ITSM, which is separately in scope under this RFP. We request you to kindly update the clauses as following - "The solution shall identify applicable compensating controls, virtual patching and exposure-mitigation options for identified exposures, shall provide the corresponding remediation/mitigation instructions and artefacts, and shall trigger and track remediation through API/webhook-based integration with the Bank's SOAR, ITSM and relevant security controls. Actual enforcement of changes on production security controls shall be performed by the respective control through the Bank's approved change-management process." Kindly confirm that compliance achieved through such SOAR/ITSM-orchestrated remediation shall not be treated as non-compliance.	Please refer addendum for revised clause Clarification: S.No 63: No Change, Please be guided by the RFP.
3371	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 61	The solution should ensure remediation actions do not disrupt business continuity	A security platform can assess and present the potential impact of a recommended remediation, but it cannot guarantee the business-continuity outcome of a change executed on the Bank's production systems, which depends on the Bank's change-management, testing and rollback processes and on the affected application's architecture. As worded, the clause places an unqualified guarantee on the bidder/OEM. We request you to kindly update the clause as following - "The solution shall provide impact assessment and risk context for recommended remediation actions, including affected assets, dependencies, prerequisites and rollback considerations, to enable the Bank to plan and execute remediation without disrupting business continuity through its change-management process."	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3372	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 55 and S.No. 56	S.No. 55 - The solution should include IOC investigation, infrastructure mapping, and threat actor identification. S.No. 56 - The visual investigation tool should integrate multiple services including WHO IS and Passive DNS.	A graph-based 'visual investigation tool' bundling WHOIS, Passive DNS and threat-actor identification is a specific feature of certain CTI/DRP investigation products and is not a CTEM platform capability; it is also available to the Bank through its threat-intelligence platform in scope under this RFP. We request you to kindly move these clauses to the Cyber Threat Intelligence/DRP or TIP scope, or update them as following - "The solution shall support investigation of identified exposures and indicators, including mapping of the Bank's internet-facing infrastructure and associated relationships (such as domains, sub-domains, certificates, DNS and WHOIS/registration data for the Bank's own digital footprint), and shall support enrichment and threat-actor context through integration with the Bank's threat-intelligence platform."	No Change, Please be guided by the RFP
3373	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 57, S.No. 58 and S.No. 67	S.No. 57 - Up on demand, the vendor should provide a dedicated Customer Success Manager as a single point of contact for onboarding and ongoing support. S.No. 58 - The vendor to provide 24/7 system support. S.No. 67 - The vendor to provide a mechanism to report security incidents identified through the platform and receive prompt response and guidance from the incident response team.	These are commercial/service clauses rather than functional specifications of the solution, and 'dedicated Customer Success Manager' and access to an 'incident response team' are named-resource and incident-response-retainer commitments that cannot be objectively evaluated in a functional compliance sheet or priced without defined limits. We request you to kindly move these clauses to the services/SLA section of the RFP and confirm - (a) whether the Customer Success Manager is required to be dedicated to the Bank full-time or is an assigned named point of contact, and whether onsite presence is expected; (b) the required support SLA and severity-wise response/resolution matrix for 24/7 support; and (c) for S.No. 67, the number of incident-response engagements per annum, whether remote or onsite, and whether these are to be priced within the subscription or as a separate retainer.	No Change, Please be guided by the RFP
3374	Functional Compliance Sheet (Appendix 1A) - CTEM	Appendix 1A - Functional Compliance Sheet (Solutions) - Continuous Threat Exposure Management (CTEM)	CTEM S.No. 65 and S.No. 66	S.No. 65 - The solution should aim to reduce Mean Time to Remediate (MTTR) and labor costs. S.No. 66 - The solution should maximize ROI from existing security tools by optimizing the security posture.	These clauses express desired business outcomes rather than verifiable functional specifications, and each carries 10 marks in a scored technical compliance sheet. Compliance cannot be objectively demonstrated or evaluated, and every bidder will necessarily mark itself compliant, which adds no discriminatory value to the Bank's evaluation. We request you to kindly either remove these clauses from the scored functional specifications, or replace them with measurable requirements as following - S.No. 65 - "The solution shall provide MTTR measurement and trending for exposures by severity, asset criticality and business unit, including SLA tracking and ageing analysis." S.No. 66 - "The solution shall provide coverage and control-effectiveness reporting across the Bank's existing security tools, identifying assets not covered by, or gaps in, existing security controls."	Please refer addendum for revised clause
3375	49	7.3.11 Cloud Security (CSPM) Tool		7.3.11 (Preamble) - Integrated cloud security solution providing a centralized and unified single-pane-of-glass view across all cloud assets, workloads, identities, configurations, applications, containers, AI services and cloud-native resources deployed across multi-cloud, hybrid-cloud and on-premises environments.	Unified visibility across cloud assets, workloads, identities, configurations, containers, Kubernetes, AI services and cloud-native resources across multi-cloud and hybrid-cloud is met from a single console. Deviation: 'on-premises environments' - CSPM assesses cloud provider control planes through APIs and has no control plane to assess for traditional on-premises infrastructure. On-premises posture is delivered through configuration/compliance benchmark auditing in the VA & VLM solution, and on-premises Kubernetes through the cloud security platform. Request the Bank confirm that on-premises security posture assessed via CIS/benchmark configuration audit in the VA & VLM solution, consolidated into the same single pane, is acceptable.	No Change, Please be guided by the RFP
3376	50	7.3.11 Cloud Security (CSPM) Tool		7.3.11.2 (10) - Key Deliverable: Incident Response & Automated Playbooks.	The platform provides prioritized findings, remediation guidance, auto-generated remediation code (IaC/CLI), and event/webhook/API triggers that drive downstream automation. Deviation: incident response playbook authoring and execution is SOAR functionality, and SOAR is separately in scope under this RFP. The CSPM tool cannot itself be the playbook execution engine. Request the Bank confirm that this deliverable will be met by publishing CSPM findings and triggers into the Bank's SOAR/ITSM, with the response playbooks built and executed there.	No Change, Please be guided by the RFP
3377	51	7.3.11 Cloud Security (CSPM) Tool		7.3.11.2 (12) - Ensure that the reports are extracted from online / warehouse storage etc. Restore the logs/data from backup for forensic investigation and as per bank requirement without any additional cost.	Findings, assessment history, audit logs and reports are retrievable on demand through the console, scheduled reports and APIs at no additional cost for the retention period applicable to the subscription. Deviation: for an OEM-managed SaaS platform there is no Bank-accessible backup media from which data is 'restored'; data is served from the live platform and its retention tier. Request the Bank (a) specify the mandated retention period, and (b) accept on-demand retrieval/export from the platform as fulfilling this requirement.	Please refer the addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3378	35 of 122	XDR	4.13	The goal is to minimize the attack surface by continuously monitoring, updating, and provide compensatory controls for vulnerabilities and exploits in the endpoints	We request to modify this clause as below "The goal is to minimize the attack surface by continuously monitoring, updating, and provide visibility for vulnerabilities and exploits in the endpoints" Justification: The term "visibility" is outcome-focused and technology-agnostic, allowing solutions to detect and report vulnerabilities through various mechanisms (signatures, behavioral analysis, real-time scanning, etc.), whereas "compensatory controls" is overly prescriptive and implies specific mitigation techniques that may not be applicable to all vulnerability types or endpoint environments. Changing to "visibility" maintains the security intent while enabling bidders to propose diverse, fit-for-purpose solutions without unnecessary implementation constraints.	No Change, Please be guided by the RFP
3379	35 of 122		12	The proposed solution must provide protection against malicious AI application tampering on the endpoints	We request to modify this clause as below "The proposed solution must provide protection against malicious applications tampering on the endpoints" Justification:The "AI" qualifier is overly specific and may exclude non-AI malware threats, creating coverage gaps. The broader term "malicious application tampering" aligns with industry-standard endpoint protection language and ensures comprehensive threat protection regardless of the attack vector or technology employed.	No Change, Please be guided by the RFP
3380	36 of 122		15	The proposed XDR solution must provide comprehensive activity data management and search capabilities, including receiving activity data in the form of telemetry, and metadata; feature for automatic query runs and email notifications; threat matching features using Boolean Logic and other criteria; and options to export, import, delete, and share saved search queries.	We request to modify this clause as below: The proposed XDR solution must provide comprehensive activity data management and search capabilities, including receiving activity data in the form of telemetry, and metadata; feature for automatic query runs and email notifications; threat matching features using Boolean Logic and other criteria; and options to export, delete, and share saved search queries. Justification:The "import" functionality is not a core operational requirement for XDR activity data management. The primary requirements are exporting queries for backup/sharing, deleting obsolete queries, and sharing queries among team members—all of which are standard XDR capabilities. Import functionality introduces unnecessary complexity, potential security/governance risks from external query sources, and is not universally supported across commercial XDR solutions, thereby limiting vendor options unnecessarily	No Change, Please be guided by the RFP
3381	36 of 122		22	The solution should offer options to leverage anti-malware and anti-spyware components stored locally on agents, or signatures stored in-the-vendor cloud	From the operational context and use cases for each deployment option, ensuring continuity of threat protection in all connectivity scenarios. By explicitly defining "when offline" (local components) and "when online" (cloud signatures), the clause removes ambiguity regarding the solution's capability to maintain protective coverage during network disconnections while leveraging updated threat intelligence when connectivity is available We request to modify this clause as below "The solution should offer options to leverage anti-malware and anti-spyware components stored locally on agents when offline, or signatures stored in-the-vendor cloud when online."	No Change, Please be guided by the RFP
3382	36 of 122		29	The solution Device Control capability must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The solution Device Control capability must support Network Devices, USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, time based device control capabilities allowing admin to define the policy specifically for the endpoint operating systems (Windows 10, 11 or higher).	We request to modify the clause as below: The solution Device Control capability must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The solution Device Control capability must support USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, allowing admin to define the policy specifically for the endpoint operating systems (Windows 10, 11 or higher)to allow the devices as required. Justification: Network Devices are typically managed through enterprise network security controls and firewalls rather than endpoint Device Control, and time-based controls create unnecessary operational complexity and maintenance overhead. The modified clause focuses on high-risk local device vectors (USB, Mobile Storage, Bluetooth, Modems) that pose direct security threats to endpoints, while allowing flexibility for organizations to enable specific devices based on business requirements.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3383	37 of 122		43	The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature or through seamless integration with a third-party sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data	We request to amend this clause as below: The proposed solution must include functionality to perform sandbox analysis of suspicious files. The sandbox environment should be provided by the bidder either as a native/inbuilt feature sandboxing solution from day 1. Sandboxing analysis should no have limited on the size or he quantity of agents sending the data. Justification: To ensure operational independence and reduce implementation complexity, the organization requires native sandbox functionality built into the core solution rather than relying on third-party integrations, which introduce external dependencies, potential single points of failure, and increase support overhead. This modification mandates that bidders deliver complete sandboxing capability as an integrated component from day 1, ensuring seamless functionality, consistent vendor accountability, and simplified maintenance and support operations without external vendor coordination.	Please refer addendum for revised Clause
3384	38 of 122		57	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	We request to amend this clause as below: The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture or 99.9% availability SLA distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead. Justification: The modification provides architectural flexibility while maintaining the Bank's core availability objective. Not all qualified SaaS vendors employ Active-Active multi-AZ architecture; however, industry-standard 99.9% SLA meets enterprise-grade requirements and enables broader vendor participation without compromising operational resilience. This alternative approach is vendor-agnostic, measurable, and backed by contractual guarantees rather than architectural prescriptions.	Please refer Addendum for revised clause
3385	37 of 122		42	The proposed solution should provide recommended actions to address and mitigate threats detected on endpoints. These remediation suggestions should be informed by forensic data collected from endpoints and detailed analysis performed by the solution to enhance threat response and resolution.	To ensure accurate cost proposals and licensing calculations, please clarify the estimated forensics data volume requirements: a) What is the expected monthly forensics data volume (in GB) that the solution must support? b) What is the planned retention period for forensics data? c) Does this volume include forensics data from all sources (endpoints, servers, cloud workloads, network) or specific sources only? This clarification will enable all bidders to calculate appropriate licensing models and provide consistent cost estimates	Details shall be shared with the successful bidder
3386	54 of 122	Cloud Security	4	The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud envirionment like AWS/Azure/GCP/Meghdoot, AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.	We request to modify this clause as below The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud envirionment like AWS/Azure/GCP/ AWS Well-architected, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports. Justification: Meghdoot is a comprehensive open-source cloud suite, but bringing it up to PSB requirements demands significant development and integration effort. To be effective, the target cloud environment must be seamless, eliminating the overhead of custom modifications.	Please refer addenudm for revised clause The solution must provide Cloud compliance scanning features to evaluate against industry benchmarks (e.g. CIS Benchmark for cloud envirionment like AWS/Azure/GCP, SOC2, HIPAA, NIST, GDPR, PCI-DSS, NYDFS) with the ability to create custom compliance standards and reports.
3387	Addition of Point as recommendation	Cloud Security	To be Added in Cloud Security	The proposed solution should also support the File scanning with no limitation on file/object type or size covering application across organisation. This should include but is not limited to Amazon Simple Storage Service (S3), Amazon FSx amd Amanzon Elastic File System.	Benefit to PSB: Comprehensive file scanning eliminates critical security blind spots across the organization's cloud storage infrastructure, ensuring no malware, ransomware, or sensitive data can be inadvertently stored in S3, FSx, or EFS without detection. By removing file type and size limitations, the solution prevents attackers from bypassing scanning through obfuscation or leveraging uncommon formats, while the multi-storage coverage consolidates security posture across diverse AWS storage services under a single unified policy. This provides unified threat visibility, enables regulatory compliance (HIPAA, PCI-DSS, GDPR), prevents data exfiltration, and protects against insider threats and supply chain compromises affecting cloud-stored data—significantly reducing the risk of ransomware attacks, compliance violations, and unauthorized data exposure.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3388	page 30 of 273	Extended Detection & Response (XDR)	5	Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Cloud (SaaS): HA Deployment aligned with the SLA, RTO & RPO (Refer Section 13). Management Console: Deployed at both Primary and Secondary sites	We request to amend this clause as below: Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Cloud (SaaS): HA Deployment aligned with the SLA, RTO & RPO (Refer Section 13). Justification: In Appendix 1A clause 27 under XDR explicitly mention for SaaS "ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead" Though it's a SaaS based the management console cannot be deployed at both primary and secondary sites.	Please refer addendum for revised clause
3389	page 31 of 273	Cloud Workload Protection Platform (CWPP)	13	Cloud (SaaS): Deployment aligned with the SLA, RTO & RPO (Refer Section 13).. Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Management Console: Deployed at both Primary and Secondary sites	We request to amend this clause as below: Cloud (SaaS): Deployment aligned with the SLA, RTO & RPO (Refer Section 13).. Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Justification: For SaaS solution the management console cannot be deployed at banks primary & secondary site	Please refer addendum for revised clause
3390	Page 38 of 122 & Page 38 of 122	XDR	22 to 35	These points are duplicate need to be removed	These points are duplicate need to be removed	No Change, Please be guided by the RFP
3391	29, 35 & 259	Sections 7.2.1, 7.2.4.1(b) & 16.21.2	Section 7.2.1 (Deception Technology): "Any agent/Enforcer/Deceptor Standalone at DC and HA, N+N, Standalone at DR." Section 7.2.4.1(b): "The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active	Deception deployment and high-availability topology	The RFP describes the Bank-side deception components as standalone in Section 7.2.1, point no.- 4, but it is also mentioned HA and N+N. We request the bank to kindly clarify that in case we're deploying the solution on-prem, whether Bank needs the solution in Standalone mode/HA mode/N+N mode. Section 16.21.2 (Decoy), point no.-8, Bank has asked that all the inline components of solution should be in HA mode with automatic failover capability. However, the deception solution is not inline. Hence, we request Bank to clarify if they need the Deception Solution in HA. We request the Bank to add on-prem solution also in addition to Cloud/SAAS+Hybrid.	Please refer addendum for revised clause
3392	45, 261 & 262	Sections 7.3.6.2(2) & 16.21.3 - Deployment and Data Retention	Section 7.3.6.2(2): "Restore the logs/data from backup for forensic investigation and as per bank requirement without any additional cost." Section 16.21.3: "Duration of the Contract (Monthly Full backup) - Long-Term Storage (LTS) - Entire Duration of the Contract." The RFP further states that applicable Monthly Full Backups shall be	Backup, restoration and log-retention requirements	We request bank to kindly confirm that if the bank will provide the storage for backup.	No Change, Please be guided by the RFP. Bidder to right size and provide all the required infrastrcuture as per RFP
3393	68	Section 7.7 - On-cloud proposed solution OEM Responsibilities, Point 10	"The OEM shall have valid ISO/IEC 27001 certification and SOC 2 Type II report."	Cloud OEM certification requirement	We request the bank to accept ISO/IEC 27001 or SOC 2 Type II or both.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3394	29, 32 & 35	Sections 7.2.1, 7.2.3 and 7.2.4.1(b)	Section 7.2.1 (Deception Technology): "Cloud (SaaS) + Hybrid" Section 7.2.3: "The solution shall be hosted through a Cloud Service Provider (CSP), either fully as a SaaS service or through a combination of CSP-hosted and Bank-hosted components." Section 7.2.4.1(b): "Deception Technology: The core Deception platform shall be deployed in the	Responsibility for providing the Cloud/SaaS environment	7.2.4.1(b) We request the bank to kindly add the on-prem implementation option also for the core component of the Deception Solution.	Please refer addendum for revised clause
3395	35 & 91	Sections 7.2.4.1(b) and 7.18.1 - Compute Infrastructure, Point 1	Section 7.2.4.1(b): "Deception Technology: The core Deception platform shall be deployed in the Cloud/SaaS environment, with the required agents, enforcers, decoys and/or honeypots deployed at the Bank's DC and DR in N+N Active-Active configuration. The Cloud/SaaS deployment shall be aligned with the applicable SLA, RTO and RPO requirements."	Hardware and VM infrastructure for Bank-hosted deception components	We request the bank to kindly add the on-prem implementation option also for the core component of the Deception Solution.	Please refer addendum for revised clause
3396	84	Breach and Attack Simulation (BAS)	Sl. No. 1 - Technical Specification	The solution should simulate Ransomware Attacks	Rationale for change: The clause as drafted is a single unqualified statement that every bidder in this category will mark compliant, so it cannot differentiate responses against the 10 marks allotted. It also does not define what constitutes a ransomware simulation. A ransomware validation exercise is only meaningful to the Bank if the platform reproduces the tradecraft ransomware operators actually use, including vulnerable driver loading to terminate endpoint protection, and does so without causing damage on production assets. The Bank is requested to replace the clause with testable criteria covering safe execution of destructive behaviours, deterministic cleanup, and kernel-level attack testing. Proposed modified clause: The proposed solution must execute structurally authentic attacks with destructive elements neutralised, and must be able to trigger destructive-technique detections without the harmful action (for example, testing volume shadow copy deletion detection without deleting the volume shadow copy). It must provide deterministic cleanup mechanisms, safe for execution on production assets, including backup, restore, and removal of all artifacts across: a. File b. Registry c. Service	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3397	84	Breach and Attack Simulation (BAS)	Sl. No. 3 - Technical Specification	The ability to simulate infiltration techniques for breaching a network or infecting a host	Rationale for change: "Infiltration techniques" is undefined and cannot be evaluated objectively. Initial access is the stage at which the Bank's email gateway, secure web gateway and web application firewall are tested, and current adversary tradecraft delivers initial access through container formats such as ISO, IMG, MSI, LNK and ZIP, followed by execution that avoids system interpreters in order to bypass AMSI, script block logging and constrained language mode. A clause that names these delivery and execution requirements allows the Bank to compare bidders on demonstrable capability rather than on a general claim. Proposed modified clause: The proposed solution must dynamically generate container-format payloads including ISO, IMG, MSI, LNK, and ZIP variants containing executables, shortcuts, or DLL hijack chains, and deliver them via uniquely generated URLs per simulation to comprehensively validate email gateway, secure web gateway, and WAF filtering against modern initial-access techniques such as ISO-LNK-DLL chains. The simulation agent must execute malicious behaviours and adversary techniques without reliance on system interpreters including PowerShell, CMD, BASH, or SH, validating control effectiveness against modern adversary tradecraft that increasingly avoids interpreter-based execution to bypass AMSI,	No Change, Please be guided by the RFP
3398	84	Breach and Attack Simulation (BAS)	Sl. No. 6 - Technical Specification	The solutions should test Security Operations Center (SOC) detection capability of bank by simulating multi-chained payloads with advanced evasion methods including DLL Hijacking, Process Injection, and PPID spoofing for breaching and infiltrating the network.	Rationale for change: The clause names only three evasion techniques and does not state that they must be executed as real behaviours on the asset rather than logged as simulated steps. SOC detection validation succeeds or fails on two things the clause does not capture: whether the payload natively performs modern evasion against the deployed control stack, and whether each technique is available in multiple procedure variants, since a detection that catches one implementation of LSASS credential dumping routinely misses six others. The Bank is requested to expand the clause so that detection coverage is validated across the attacker variant space. Proposed modified clause: The simulation payload execution must natively perform the following techniques as executed behaviours against the deployed control stack: a. EDR unhooking (NTDLL unhooking, direct and indirect syscalls) b. Reflective DLL injection c. Process hollowing d. PPID spoofing e. Command-line argument spoofing f. Fileless in-memory execution For each in-scope MITRE ATT&CK technique, the proposed	No Change, Please be guided by the RFP
3399	84	Breach and Attack Simulation (BAS)	Sl. No. 7 - Technical Specification	The solution should have the ability to create custom use cases / simulations attacks according to bank's requirement.	Rationale for change: As drafted the clause is satisfied by a script upload field or by a vendor professional services engagement, both of which leave the Bank dependent on the OEM for every new scenario and carry recurring cost. For the Bank's own security team to build scenarios for proprietary applications and internal workflows, the clause should require a user interface driven attack creator with named configurable parameters. Proposed modified clause: The proposed solution must provide a UI-driven attack creator enabling customer security teams to design custom multi-stage simulations with configurable name, description, MITRE category, execution privileges (User/Admin), payload type (DLL/EXE/Service/ISO/MSI/LNK), and chained secondary behaviours supporting organisation-specific scenario testing for proprietary applications, internal workflows, and bespoke attack hypotheses.	No Change, Please be guided by the RFP
3400	84	Breach and Attack Simulation (BAS)	Sl. No. 8 - Technical Specification	The solution must allow the execution of simulations on multiple agents simulataneously. An attack chain must be executed on multiple endpoints agents at the same time to provide unique attack specific insights across the deployed agents in the organisation.	Rationale for change: The clause states the requirement for simultaneous execution but does not exclude sequential execution presented as a single campaign, which is how several solutions in this category operate. It also does not address the operational prerequisites for running simulations across a bank-scale estate: the agent must be deployable at scale through Group Policy or golden image, must run silently so that branch and business users are not alerted or disrupted, and must update centrally without re-imaging or desk visits. The Bank is requested to make both the concurrency model and the deployment model explicit. Proposed modified clause: The proposed solution must execute a single coordinated attack campaign across multiple agents, business units, and geographies simultaneously, not sequentially (i.e. One Kill chain, run on multiple Endpoint Targets at the same time), producing independent per-agent evidence consolidated into a unified campaign report. Solutions that walk through agents one-by-one cannot realistically validate enterprise-scale concurrent compromise scenarios. The simulation agent must be a lightweight software package suitable for enterprise mass-deployment via Group Policy Object (GPO), golden image baking, or standard endpoint management tooling, requiring no per-host configuration post-installation,	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3401	84	Breach and Attack Simulation (BAS)	Sl. No. 11 - Technical Specification	The solution should support technical integrations with bank's existing solutions (e.g., SIEMs, ticketing systems, log management, Firewalls, automation/orchestration, analytics solutions, threat intelligence solutions, etc.)	Rationale for change: "Should support technical integrations" is unverifiable and is routinely answered with roadmap commitments or bespoke development quoted after award. For closed-loop validation, where a simulation result is correlated against the alert raised in the Bank's SIEM and a ticket is created automatically, the Bank needs a documented API, automation tooling and pre-built connectors available at the time of bid. The Bank is requested to make the integration requirement specific and verifiable. Proposed modified clause: The proposed solution must expose a RESTful API with publicly available OpenAPI documentation, provide an open-source CLI and SDK for automation, and ship pre-built integrations with major SIEM, SOAR, ITSM, EDR, firewall, and email gateway vendors to enable closed-loop validation of alerts, automated ticket creation, and detection correlation.	No Change, Please be guided by the RFP
3402	30	RFP - 7.2 Solution & Services Deployment Model and Their HA Requirement 7.2.1 Solutions – Master Deployment Matrix	6. Network Detection & Response (NDR)	Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Management Console: Deployed at both DC and DR	Different NDR solution works on different redundancy deployment methodology (I.e Active - Active or Active - Passive). Request bank to modify the clause as: Bank Location: Broker/Aggregator/Collector/Enforcer: HA, N+N, Active-Active/Passive at DC and HA, N+N, Active-Active/Passive at DR. Management Console: Deployed at both DC and DR	Please refer addendum for revised clause
3403	45	RFP - Scope of Work 7.3.5 Network detection and response (NDR)	7.3.5.1 Modules, Architecture & Deployment:	Pt 2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Generally NDR solutions are deployed with sole purpose of doing network analysis, threat detection & response and does not have native 2FA capability, so request bank to remove this point. As an alternate as proposed in same point, proposed NDR solution can be integrated with bank's existing MFA solution.	Please refer addendum for the revised clause
3404	49	RFP - Scope of Work 7.3.10 Application security testing Tool	7.3.10.1 Modules, Architecture & Deployment:	Pt 2. The proposed solution should have Two-Factor Authentication (2FA) and should also be capable of integrating with the bank's existing Multi-Factor Authentication (MFA) solution.	Generally AST solutions are deployed with sole purpose of scanning the source code, web, api etc and does not have native 2FA capability, so request bank to remove this point. As an alternate as proposed in same point, proposed AST solution can be integrated with bank's existing MFA solution.	No Change, Please be guided by the RFP
3405	110	RFP - 10.2 Eligibility Evaluation Criteria	OEM Evaluation Criteria	Pt 19. The proposed OEM SIEM Solution with a minimum capacity of 30,000 EPS or 1.2 TB/day shall have been successfully implemented on cloud in one (1) in India.	For wider participation, we request bank to amend the clause as: The proposed OEM SIEM Solution with a minimum capacity of 5,000 EPS or.2 TB/day shall have been successfully implemented on cloud in any one (1) Govt/PSU customer in India. OR The proposed OEM SIEM Solution with a minimum capacity of 10,000 EPS or.4 TB/day shall have been successfully implemented on cloud in one (1) in India.	Please refer addendum for revised clause.
3406	112	RFP - 10.2 Eligibility Evaluation Criteria	OEM Evaluation Criteria	Pt 20. The proposed OEM solution should have been implemented in at least one BFSI is to be submitted for the following solutions: NDR	For wider participation, we request bank to amend the clause as: The proposed OEM solution should have been implemented in at least one BFSI / Govt is to be submitted for the following solutions: NDR	Please refer addendum for the revised clause
3407	260	RFP - 16.21.2 Volumetrics- Solution-wise Requirements	12. Application Security Testing Tool	All the inline components of the solution must operate in high availability mode. In the event of any component failure, the system should automatically initiate failovers within seconds, ensuring uninterrupted functionality without requiring manual intervention.	Application Security Testing as a technology in general works at developemnt/pre-production/UAT stage only. And hence as a solution there is no need of high availability mode. Same has already been updated in this RFP (as solution is asked in standalone at both DC & DR). So, request bank to deleted this clause.	No Change, Please be guided by the RFP. The bidder must design the solution to fully comply with the RFP requirements, ensuring that in case of a failover, the system meets the defined SLA for availability, RTO, and RPO. The bidder is required to adhere to the deployment requirements outlined in the RFP when designing and proposing the solution architecture.
3408	40	APPENDIX 1A Functional Compliance Sheet (Solutions)	Network Detection & Response (NDR)	Pt 8. Proposed solution should generate a root cause analysis, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets.It should provide a platform for easier investigation like visual graphical view and timeline of the attack and it should support tagging of MITRE tactics, techniques and procedures used by the attacker in alerts and incidents.	We reqeust bank to amend the clause: Proposed solution should generate a root cause analysis / incident management, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets.It should provide a platform for easier investigation like visual graphical view and timeline of the attack and it should support tagging of MITRE tactics, techniques and procedures used by the attacker in alerts and incidents.	Please refer addendum for the revised clause
3409	40	APPENDIX 1A Functional Compliance Sheet (Solutions)	Network Detection & Response (NDR)	Pt 13. The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	As bank has asked for on-premise solution for NDR, on the contrary, this clause asks for cloud-native SAAS ask. So, we kindly request bank to delete this clause.	Please refer Addendum for revised clause
3410	42	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 3. The solution must be able to analyse a wide array of programming languages including Java,.Net, C/C++, Objective-C, Android, PHP, COBOL, Ruby, Swift, HTML 5, Scala, APEX, TypeScript, Go, Kotlin and ABAP etc but not limited to these alone	Considering the future requirements of AI in Secure Code Development and most of the development is moving towards AI generated code using AI supported languages. So it is very important for bank to have coverage around this as well and will recommend to incorporate AI supported languages like "R, Ada, Solidity, Bash, Groovy, Rust, Perl", but not limited to these alone.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3411	42	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 24. Solution should support Machine learning and Analysis based on the archived results	ML capability is important, but it is very important to have coverage around AI based code as well. And will recommend bank to consider: The solution should have the capability to scan AI generated code. The solution should be able to integrate with AI coding agent via MCP	No Change, Please be guided by the RFP
3412	43	APPENDIX 1A Functional Compliance Sheet (Solutions)	Application Security testing tool	Pt 32. The solution should be able to support Composition Analysis: Identify the opens source components used in the application. Vulnerabilities & outdated version Licensing risk associated with the components	Bank is looking for Software composition analysis and asked for identifying the open source component and licensing risk. But this limited information is not enough for bank to secure themselves with rapidly increasing supply chain attacks and we will highly recommend to consider following as well: SCA system must catalogue open source components from Maven, NPM, and Nuget. SCA system has to be able to generate a Bill of Materials for an application. Solution should have the ability to continuously monitor the scanned components & notify if there are any zero day attacks without performing the rescan. Solution should Catalog, Store, and Audit SBOMs (both cycloneDx & SPDX) generated for in-house developed software applications and COTS applications.	No Change, Please be guided by the RFP
3413	30	7.2 Solution & Services Deployment Model and Their HA Requirement 7.2.1 Solutions – Master Deployment Matrix	Sl. No. 8	Vulnerability assessment (VA) & vulnerability lifecycle management Bank Location: Standalone at DC and Standalone at DR. Management Console: Deployed at both DC and DR	Requesting clarifications if standalone management console in DR will be live or will be on standby ?	Please refer addendum for revised clause
3414	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 1 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall be deployable entirely on-premises and shall not require any cloud-hosted component, external service, or Internet connectivity for its core functionality, scanning, management, reporting, analytics, or product capabilities.	Requesting change to: The proposed solution shall be deployable entirely on-premises or hosted on MeitY cloud or Meity empanelled cloud environment. No data shall be shared with the platform/cloud outside India geolocation.	Please refer addendum for the revised clause
3415	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 3 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall be software-based and fully deployable on the hardware infrastructure proposed by the Bidder.	Requesting change to: The proposed solution shall be software-based and fully deployable on the hardware infrastructure or should support hybrid- on-premise architecture with management-console or scanners on on-premise and analytics components on MeitY/MeitY-emapanneled cloud proposed by the Bidder.	No Change, Please be guided by the RFP
3416	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 9 of Vulnerability Assessment & vulnerability lifecycle Management	Each scanning engine shall support web application security assessment together with traditional infrastructure vulnerability and configuration/compliance assessment. The solution shall identify vulnerabilities, missing patches, insecure configurations, and compliance deviations, and generate comprehensive reports containing risk severity, evidence of findings, affected assets, and remediation recommendations to support security governance, audit, and regulatory compliance.	Requesting to confirm that if DAST specs are specifically provided for web-application's VAPT, then what is the scope of "web-application" scanning in this spec? Also requesting to share the total number of web-applications considered in the scanning scope.	No Change, Please be guided by the RFP
3417	47	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 18 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall support both active and passive asset discovery and vulnerability assessment/scanning.	Requesting change to: The proposed solution shall support both active and/or passive asset discovery and vulnerability assessment/scanning.	No Change, Please be guided by the RFP
3418	48	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 27 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall support both active and passive techniques for vulnerability detection, where applicable.	Requesting change to: The proposed solution shall support both active and/or passive techniques for vulnerability detection, where applicable.	No Change, Please be guided by the RFP
3419	48	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 33 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall support deployment and lifecycle management of scanning agents without dependency on cloud-hosted services.	Requesting change to: The proposed solution shall support deployment and lifecycle management of scanning agents.	No Change, Please be guided by the RFP
3420	48	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 34 of Vulnerability Assessment & vulnerability lifecycle Management	The proposed solution shall assess Active Directory security posture and identify misconfigurations, privilege risks, insecure policies, and exposure of critical directory services.	Requesting to clarify that this spec is already addressed in IDTR then what is the requirement of it in VM solutin?	No Change, Please be guided by the RFP
3421	49	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 74 of Vulnerability Assessment & vulnerability lifecycle Management	The solution shall support offline signature and plugin updates for deployment in isolated or air-gapped environments.	Requesitng to remove this spec because if the cloud-based solution is offered and where cloud is hosted on MeitY cloud or MeitY empanneled cloud then questions related to air-gap environment doesn't arise.	No Change, Please be guided by the RFP
3422	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 81 of Vulnerability Assessment & vulnerability lifecycle Management	The solution shall support password-protected and/or digitally signed reports with configurable retention and archival.	Requesting change to: The solution must support secure, encrypted report distribution (including native PGP encryption) and enforce strict role-based access controls (RBAC) for report viewing. Additionally, the platform must provide configurable cloud-based data retention policies alongside automated options to archive historical scan data and reports to external storage	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3423	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 87 of Vulnerability Assessment & vulnerability lifecycle Management	AI-Assisted Vulnerability Triage and Reporting: The proposed solution shall provide AI-assisted vulnerability triage, including risk/verdict assessment and supporting rationale, along with automatically generated executive-level vulnerability summaries. Such AI processing shall be deployable entirely within the Bank's on-premises environment or an equivalent Bank-controlled environment, ensuring that source code, vulnerability data, scan results, credentials, and other Bank data are not transmitted to or processed by external/public AI services.	Requesting change to: The solution must provide AI-generated risk summaries and plain-language vulnerability briefs that automatically fuse asset criticality, technical findings, and real-world threat telemetry (such as CISA KEV and EPSS data) to streamline IT triage. If cloud analytics are utilized to run these machine learning models, the solution vendor must guarantee that all data is isolated within dedicated, bank-authorized cloud regions, employing strict data privacy frameworks that ensure source code, credentials, and raw scan parameters are explicitly excluded from public AI training models or multi-tenant public AI services	Please refer addendum for revised clause
3424	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 88 of Vulnerability Assessment & vulnerability lifecycle Management	Unified, correlated findings intelligence. Every scanning engine — across web, API, network and host, cloud, containers, mobile, source code, device configuration and identity — reports into a single normalized findings model..	Requesting clarification on why unified reporting is asked as the ASM, VM, DAST solutions are considered separately.	No Change, Please be guided by the RFP
3425	50	APPENDIX 1A Functional Compliance Sheet (Solutions)	sl. No. 90 of Vulnerability Assessment & vulnerability lifecycle Management	Mobile Application Security Testing: The proposed solution shall support static security analysis of Android and iOS mobile application packages, including APK/AAB and IPA formats, and shall provide security assessment mapped to recognized mobile application security standards and methodologies such as OWASP MASVS and MASTG.	Requesting clarification for the spec as the ask is for DAST or MAST solution.	No Change, Please be guided by the RFP
3426	87	Anti Phishing Services	17.1	Solution should detect at the earliest point in the attack, post initial compromise as the attacker is first attempting to move laterally and escalate privilege.	Since this section is focused on Anti-Phishing, we understand that the objective is to identify suspicious activity following a successful phishing or account-compromise event. Network-level lateral movement and deception capabilities may be addressed by other security controls. We request the Bank to clarify whether this clause may instead focus on early post-compromise user activity visibility for the Bank's most critical users. " The solution should support early identification and investigation of suspicious user activities associated with potential account compromise following phishing or other email-originated attacks, with enhanced user activity monitoring for up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles."	Please refer to the relevant Addendum for updated specfications
3427	87	Anti Phishing Services	17.4	Solution must provide robust supply chain and AI/ML-driven contact chain analysis capabilities to identify and defend against socially engineered, impersonated, or BEC attacks.	As compromise of trusted suppliers and partners is an important source of BEC and phishing risk, we request the Bank to clarify whether the existing supply-chain requirement should explicitly include behavioural analysis of supplier/partner communication patterns to identify attacks originating from compromised trusted accounts. " Solution must provide robust supply-chain and AI/ML-driven contact-chain and behavioural analysis capabilities to identify and defend against socially engineered, impersonated or BEC attacks, including threats originating from compromised or impersonated supplier/partner accounts."	Please refer to the relevant Addendum for updated specfications
3428	87	Anti Phishing Services	18	Solution must proactively analyze suspicious URLs using dynamic/behavioral analysis to prevent the spread of malware and other threats.	The RFP separately addresses URL analysis and post-delivery remediation. We request clarification whether these requirements are intended to provide continuous protection throughout the email threat lifecycle, including pre-delivery analysis, click-time URL protection and post-delivery detection/remediation. " Solution must provide continuous protection across the email threat lifecycle, including pre-delivery threat detection, real-time/click-time inspection of suspicious URLs, and post-delivery detection and automated remediation of threats that are subsequently determined to be malicious."	Please refer to the relevant Addendum for updated specfications
3429	88	Anti Phishing Services	19.7	Solution must be able to offer a comprehensive portal that allows users to access information and metadata on events/incidents, facilitating network threat forensics for thorough investigation and analysis of potential security breaches or incidents.	To strengthen investigation of phishing-led incidents involving executives and other critical users, we request clarification whether the existing forensic portal requirement may also include contextual user and endpoint activity for a limited population of Bank-identified critical/high-risk users. " Solution must offer a comprehensive investigation portal providing information and metadata on events/incidents for forensic analysis. For up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, the portal should additionally provide contextual user and endpoint activity, including relevant application, file and user-action details, to support investigation of potential phishing-led compromise."	Please refer to the relevant Addendum for updated specfications
3430	88	Anti Phishing Services	19.9	Solution must empower security operations and incident responders to automate the identification, remediation, and sharing of phishing threats, streamlining the process of detecting, addressing, and disseminating information about potential phishing attacks for improved response and mitigation.	To improve SOC investigation efficiency, we request clarification whether the existing phishing identification and remediation requirement should include centralized attack context showing why a message was identified as malicious, the users targeted, associated threat indicators and remediation status. " Solution must empower security operations and incident responders to automate identification, investigation, remediation and sharing of phishing threats, and should provide centralized contextual visibility into the users targeted, associated threat indicators, detection rationale, attack characteristics and remediation actions."	Please refer to the relevant Addendum for updated specfications

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3431	88	Anti Phishing Services	19.1	Solution must provide incident responders with real-time analytics and visibility into email-based attacks targeting the organization.	Email-based attacks against executives and privileged users may require additional context after delivery to determine whether a targeted user has subsequently performed suspicious activity. We request the Bank to clarify whether real-time investigation visibility may include relevant user activity context for up to 100 Bank-identified critical/high-risk users. " Solution must provide incident responders with real-time analytics and visibility into email-based attacks targeting the organization. For up to 100 Bank-identified critical/high-risk users, the solution should additionally provide contextual visibility into suspicious user activities associated with potential phishing or account compromise, including relevant user, endpoint, application and file activity."	Please refer to the relevant Addendum for updated specfications
3432	88	Anti Phishing Services	19.23	Solution must have simplicity of evaluation and additional visibility into internal traffic and other communication channels can reduce risk, and baseline user activity to detect suspicious behavior.	The existing clause already seeks baselining of user activity to detect suspicious behaviour. We request the Bank to clarify the intended depth and scope of this capability and whether enhanced monitoring may be applied to a focused population of up to 100 Bank-identified critical/high-risk users, where deeper visibility provides the greatest security value. " Solution must provide additional visibility into relevant internal activity and communication channels to reduce risk and baseline user activity to detect suspicious behaviour. Enhanced user and data activity monitoring should be provided for up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, with configurable detection policies for suspicious, anomalous or policy-violating activities."	Please refer to the relevant Addendum for updated specfications
3433	90	Anti Phishing Services	19.7	Solution must provide protection against harassment mail and mitigate the risks associated with emails from unknown senders specifically for executives or VIPs, safeguarding them from potential threats and ensuring their email communication remains secure.	Since this clause already provides enhanced protection for executives/VIPs, we request the Bank to clarify whether such enhanced protection should extend beyond receipt of suspicious email to investigation of risky user and data activities that may occur following phishing or account compromise, for a limited set of the Bank's most critical users. "Solution must provide protection against harassment mail and mitigate risks associated with emails from unknown senders specifically for executives or VIPs. For up to 100 Bank-identified critical/high-risk users, including executives, privileged users and other sensitive roles, the solution should additionally provide enhanced visibility into risky user and data activities following suspected phishing or account compromise, including relevant file movement, web/upload activity, removable-media activity and other supported data-transfer channels."	Please refer to the relevant Addendum for updated specfications
3434	52	Idendity Threat Detection and Response (ITDR)	1.7	Detect and respond to active threats with high fidelity (low false positives and false negatives).	The Bank has separately specified a comprehensive deception platform for detection of active attacker activity, reconnaissance and lateral movement. We understand that the intent of this clause within ITDR is therefore to complement those controls with focused monitoring of the Bank's most critical identities. Considering that enhanced user-activity monitoring is most relevant for high-risk personnel such as executives, privileged users and other critical users, we request the Bank to kindly clarify whether this requirement may be read as follows: " Identity Threat Detection Solution should provide high-fidelity detection and response for risky or anomalous user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, to identify activities associated with careless, malicious or compromised users. "	No Change, Please be guided by the RFP
3435	52	Idendity Threat Detection and Response (ITDR)	1.8	Provide contextual information—who, what, when and how—to inform all stages of the attack chain.	The Bank has already sought attack-lifecycle visibility under the separate deception requirements. For ITDR, we understand that additional value would be derived from detailed user-centric context for the Bank's most critical identities, enabling investigation of risky activity performed by such users. We request the Bank to kindly clarify whether this requirement may be read as follows: " Identity Threat Detection Solution should provide contextual information—who, what, when, where and how—around risky user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, to support investigation and response."	No Change, Please be guided by the RFP
3436	52	Idendity Threat Detection and Response (ITDR)	1.9	Provide deep insights into both the potential and used privilege escalation and lateral movement steps in an attack.	Privilege escalation and lateral-movement visibility is already substantially addressed under the separately specified deception solution, including attacker lifecycle visibility, MITRE ATT&CK mapping, deceptive attack paths and detection of lateral movement. To avoid duplication while retaining complementary investigation capability for high-risk identities, we request the Bank to kindly clarify whether this requirement may be read as follows: "Identity Threat Detection Solution should provide deep insights into activities performed by up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, covering application usage, file and data movement, endpoint activity and other risky behaviours to support investigation of compromised, malicious or negligent user activity."	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3437	52	Idendity Threat Detection and Response (ITDR)	2.9	Detect all types of attack vectors including pre-attack reconnaissance, zero-day attacks, privilege escalation prevention, lateral movement and data theft.	Pre-attack reconnaissance, lateral movement, malware/attack behaviour and attacker lifecycle visibility are already covered under the Bank's separate deception specifications. We understand that the complementary requirement under ITDR should focus on identity/user risk and potential data-loss activity for the Bank's most critical users rather than duplicate the deception control. We request the Bank to kindly clarify whether this requirement may be read as follows: " Identity Threat Detection Solution should detect risky user and data activities for up to 100 critical/high-risk users identified by the Bank, including executives, privileged users and other sensitive roles, including suspicious application usage, unauthorized access or movement of sensitive information, removable-media activity, web-based transfer, cloud synchronization and other potential data-exfiltration activities."	The Clause is applicable only to idendity related threat vector only. The volumetrics is provided in the RFP and should be complied
3438	52	Idendity Threat Detection and Response (ITDR)	2.10	Detect multiple attacks simultaneously.	We understand the intent is to ensure that the solution is not restricted to investigation of a single event at a time. Since active attacker detection is separately covered by the deception solution, we request that this clause be clarified in terms of concurrent monitoring and investigation of risky activities across the Bank's designated critical-user population: "Identity Threat Detection Solution should be capable of detecting and investigating multiple risky user and data activities simultaneously across up to 100 critical/high-risk users and their monitored endpoints."	No Change, Please be guided by the RFP
3439	52	Idendity Threat Detection and Response (ITDR)	3.2	Provide unified presentation of both source- and target-based telemetry data in a timeline view.	The Bank has separately specified end-to-end attacker visibility and behavioural analysis under the deception solution. For ITDR investigations involving critical identities, a chronological user-activity view would provide complementary evidence of actions performed by the user. We request the Bank to kindly clarify whether the requirement may be read as follows: " Identity Threat Detection Solution should provide a unified chronological timeline of user- and endpoint-based activity telemetry for up to 100 critical/high-risk users identified by the Bank to support investigation of risky or suspicious user activity."	No Change, Please be guided by the RFP
3440	52	Idendity Threat Detection and Response (ITDR)	3.3	Correlate identity-related telemetry from relevant source and target systems to identify and investigate identity compromise, privilege escalation, credential abuse and lateral movement.	Privilege escalation and lateral-movement detection are already addressed through the separately specified deception controls. To provide complementary investigation capability for the Bank's highest-risk identities, we request the Bank to clarify whether this clause may focus on correlation of user, endpoint, application and data activity for the designated critical-user population: " The solution shall support correlation of user, endpoint, application and data-activity telemetry for up to 100 critical/high-risk users identified by the Bank to identify and investigate suspicious user behaviour, sensitive-data movement, policy violations and potential data-exfiltration activities."	No Change, Please be guided by the RFP
3441	52	Idendity Threat Detection and Response (ITDR)	3.4	Integrate with compatible endpoint/extended detection solution to capture screen recordings or screenshots during active attacker sessions as advanced forensic evidence.	The Bank has separately specified attacker-session and forensic visibility through the deception platform. Within ITDR, we understand that visual evidence is intended to strengthen investigation of high-risk user activity. We request the Bank to kindly clarify whether the requirement may be read in an outcome-based manner for the designated critical-user population: " The Identity Threat Detection Solution should support screenshots, screen capture or equivalent visual evidence of relevant activity for up to 100 critical/high-risk users during suspicious or high-risk user sessions, as part of forensic investigation and evidence collection."	Please refer addendum for revised clause.
3442	52	Idendity Threat Detection and Response (ITDR)	3.5	Integrate with compatible network detection solution to support collection of PCAP data for network-level incident visibility.	The requirement for PCAP is network-centric and does not directly relate to identity posture or focused user-activity monitoring. Further, the Bank's separate deception specifications already require high-interaction decoys, recording of attacker activities, traffic/behaviour visibility, forensic investigation and integration with network/security technologies. To avoid duplication of network-level forensic controls across two solution categories, we request the Bank to kindly delete this clause from the ITDR section.	Please refer addendum for revised clause.
3443	52	Idendity Threat Detection and Response (ITDR)	3.6	Push incident data into SIEM/XDR or SOAR technologies via integrations for improved incident management.	We understand that the objective is to ensure relevant ITDR alerts and investigation context are available to the Bank's SOC ecosystem. For the enhanced monitoring of designated critical users, we request the Bank to kindly clarify whether alerts and activity information may be shared through supported integrations or APIs as follows: " Identity Threat Detection Solution should make alerts and relevant incident/activity data for the monitored critical-user population available to SIEM/XDR, SOAR or other supported security platforms through integrations or APIs for improved incident management."	The proposed solution hould be integrated with SIEM/XDR or SOAR technologies for sharing the incident data via supported integrattion or APIs
3444	52	Idendity Threat Detection and Response (ITDR)	3.7	As part of forensic data collection, include detailed attack path information including protocols leveraged during the attack.	Detailed attack-path and attacker-behaviour visibility is already sought under the separate deception specifications, including deceptive attack paths, MITRE ATT&CK mapping and forensic investigation. To avoid overlap while retaining complementary evidence for investigations involving the Bank's critical identities, we request the Bank to kindly clarify whether the requirement may be read as follows: " Identity Threat Detection Solution should, as part of forensic data collection for up to 100 critical/high-risk users, include detailed user-activity information such as applications used, files accessed, data movement, destination channels and other relevant endpoint activity associated with the incident."	Please refer addendum for revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3445	52	Idendity Threat Detection and Response (ITDR)	3.8	Collect user and computer information from Active Directory as part of forensic data gathering to enhance context and assess risk exposure.	We understand that directory information is required to enrich investigations with user and computer context. We request the Bank to clarify that enterprise identity context may be maintained for the overall identity population, while detailed endpoint/user-activity telemetry may be applied to the Bank's designated critical-user population: " Identity Threat Detection Solution should use relevant user and computer identity information to enhance forensic context and risk assessment, and should correlate such context with detailed endpoint/user-activity telemetry for up to 100 critical/high-risk users identified by the Bank."	Please refer addendum for revised clause
3446	52	Idendity Threat Detection and Response (ITDR)	3.9	Detect an adversary's attempt to move laterally toward key assets using as many Windows, Mac or Linux hosts as possible without requiring a persistent agent.	The Bank's separate deception specifications expressly require detection of lateral movement, reconnaissance, credential theft and malicious activity using agentless and/or agent-based deception techniques across the enterprise. The present clause therefore duplicates a capability already being procured under the Deception section. To avoid overlapping scope and duplicate controls, we request the Bank to kindly delete this clause from the ITDR section.	Please refer addendum for revised clause
3447	52	Idendity Threat Detection and Response (ITDR)	3.10	Collect AD user/computer information for forensic context and detect at the earliest point post initial compromise as the attacker first attempts lateral movement and privilege escalation.	Early detection of lateral movement and privilege-escalation activity is substantially covered under the Bank's separate deception requirements. To retain a complementary identity/user-risk objective without duplicating the deception scope, we request the Bank to kindly clarify whether this clause may focus on early detection of risky activity among the designated critical-user population: " Identity Threat Detection Solution should use relevant identity context and detect risky user behaviour at the earliest possible point for up to 100 critical/high-risk users, based on monitored endpoint activities and configured detection policies, enabling investigation and response before such activity results in significant data loss or business impact."	Please refer addendum for revised clause
3448	52	Idendity Threat Detection and Response (ITDR)	3.11	Collect AD user/computer data during forensic gathering while ensuring all deception techniques remain hidden from legitimate users.	The requirement to ensure deception techniques remain hidden from legitimate users is inherently a deception-platform capability. The Bank has already included comprehensive deception requirements covering lures, breadcrumbs, fake credentials, deceptive assets, attacker engagement and techniques designed to remain undetected by attackers. We therefore request the Bank to kindly delete this clause from the ITDR section to avoid duplication.	Please refer addendum for revised clause.
3449	2	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	10	OEM shall ensure compliance of the complete proposed solution & platform with RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and all applicable regulations throughout the contract period.	We request the Bank to clarify that the OEM is required to maintain applicable security, privacy and regulatory controls relevant to the services provided and furnish available compliance/assurance documentation, while the overall regulatory compliance obligation of the Bank remains subject to the Bank's deployment, configuration and usage of the service. " OEM shall maintain security, privacy and compliance controls applicable to the proposed hosted service and shall provide available independent assurance reports, certifications and relevant compliance documentation to support the Bank's obligations under applicable RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeitY and other applicable regulatory requirements."	Please refer addendum for revised clause
3450	2	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	20	The Service uptime agreement for the proposed solution on cloud should have monthly uptime commitments and have transparent monthly credit calculations in case of uptime not being met for any services.	We understand that published/contracted OEM hosted-service SLA commitments and corresponding service-credit methodology shall meet this requirement. Kindly confirm.	No Change, Please be guided by the RFP
3451	3	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	29	Solution provider should provide the design and process for data deletion in the scope of an independent audit and that the operational effectiveness of these controls is tested. The report for the same should be submitted to bank as and when asked by bank.	For a globally operated hosted security service, control effectiveness is generally evidenced through independent assurance reports such as SOC 2 Type II and documented data-retention/deletion controls. We request the Bank to permit such independent assurance documentation instead of requiring a separate bespoke data-deletion audit report. " Solution provider shall maintain documented secure data-retention and deletion controls. Compliance may be demonstrated through applicable independent third-party assurance reports/certifications (such as SOC 2 Type II or equivalent) and documented data-retention/deletion policies made available subject to OEM confidentiality requirements."	Please refer addendum for the revised clause
3452	4	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	41.3	Independent audit for testing effectiveness of secure data removal, such that data is rendered permanently inaccessible. (Including any backup or distributed online media).	We request the Bank to accept independently audited secure deletion and media-management controls, together with documented retention/deletion periods, rather than requiring a customer-specific audit of all backup and distributed media. " The OEM shall maintain secure data deletion, media handling and backup-retention controls designed to render customer data inaccessible in accordance with documented retention schedules. Effectiveness may be evidenced through independent assurance reports such as SOC 2 Type II/ISO 27001 or equivalent and relevant OEM security/privacy documentation."	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3453	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	47.2	Bank shall have an option to implement 'Bring Your Own Key' as and when required.	The proposed service protects data at rest and in transit using strong encryption; however, customer-managed infrastructure encryption keys are not a standard capability of the hosted anti phishing service. We request deletion of the BYOK requirement, or acceptance of OEM-managed enterprise-grade encryption and key-management controls. " Requested Action: Delete the BYOK requirement. Alternatively: 'Data processed/stored by the hosted service shall be protected using industry-standard encryption in transit and at rest, with secure OEM-managed key-management controls subject to independent security assurance.'"	Please refer addendum for the revised clause
3454	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	49	Web Application Firewall shall be implemented on the cloud for Web based applications. WAF application signature should be updated and reviewed regularly. The Report shall be submitted to bank on a periodic interval.	Since the proposed platform is an OEM-managed hosted security service, underlying WAF technology, signatures and configurations form part of the OEM's internal security architecture and may not be exposed as customer-specific reports. We request the Bank to accept periodic VAPT/penetration-test assurance or equivalent independent security assessment evidence covering the hosted application instead of WAF signature reports. " The hosted web application/platform shall be protected through appropriate application-security controls. The OEM shall conduct periodic vulnerability assessment and penetration testing/security assessments and, subject to confidentiality restrictions, provide an executive summary/attestation or applicable independent assurance evidence to the Bank on request. Customer-specific WAF signature reports shall not be mandatory."	Please refer addendum for revised clause
3455	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	52	The systems in cloud infrastructure should be periodically updated with the latest anti-malware signatures, the bidder shall submit the periodic report on the same with bank.	For an OEM-managed hosted security service, infrastructure anti-malware/endpoint controls are centrally managed and independently audited. We request the Bank to accept OEM security assurance and vulnerability/malware-control attestations rather than periodic host-level signature reports. " The OEM shall maintain appropriate malware protection, vulnerability management, patching and security monitoring controls for the hosted infrastructure. Compliance may be evidenced through independent assurance reports/certifications and applicable security-control attestations instead of customer-specific anti-malware signature update reports."	Please refer addendum for revised clause
3456	5	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	53	Data Loss Governance and risk management framework shall be defined by bidder for workload on the cloud and same shall be shared with bank on periodic basis. Data loss prevention controls should be implemented to secure the data in the cloud environment from unauthorized or inadvertent exfiltration.	We request clarification that the requirement is intended to ensure protection against unauthorized/inadvertent data exfiltration through the proposed service and appropriate security controls for hosted customer data, rather than requiring disclosure of the OEM's internal cloud governance framework. " The proposed solution shall provide configurable controls to identify and prevent unauthorized or inadvertent transmission/exfiltration of sensitive information through any channels. The OEM shall maintain appropriate access control, encryption and data-protection controls for customer data processed within the hosted service and provide applicable assurance documentation on request."	Please refer addendum for revised clause
3457	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	81	Log generation, storage and review process should be certified by CERT IN empaneled auditor, report for the same shall be submitted by bidder as and when required by bank.	For global SaaS/POD services, security logging and monitoring controls are typically independently audited under recognized assurance frameworks. We request the Bank to accept SOC 2 Type II/ISO 27001 or equivalent independent assurance in lieu of a mandatory CERT-In-empanelled audit of the OEM's internal log-generation/storage/review process. " The OEM shall maintain documented security logging, monitoring, retention and review controls. Effectiveness shall be evidenced through applicable independent third-party assurance reports/certifications such as SOC 2 Type II, ISO 27001 or equivalent. CERT-In-empanelled audit may be required only for bidder-managed components deployed specifically within the Bank environment, where applicable."	Please refer addendum for the revised clause
3458	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	82.5	IT Act 2000 & its amendments, and other Acts/Regulatory guidelines.	Kindly clarify that the OEM must comply with legal/regulatory requirements applicable to it as the provider of the proposed hosted service and provide reasonable documentation to support the Bank's compliance obligations. " OEM shall comply with applicable legal and regulatory obligations relevant to its provision of the proposed service and shall provide available security/privacy/compliance documentation reasonably required to support the Bank's applicable obligations."	Please refer addendum for the revised clause
3459	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	83	CERT IN Empaneled auditor report's is required for the following:	We request the Bank to permit internationally recognized independent assurance reports/certifications for OEM-managed hosted services. CERT-In empanelled audit reports may remain applicable to India-specific bidder-managed/on-premises components where such audit is feasible and required. " For OEM-managed hosted/SaaS services, independent assurance reports/certifications such as SOC 2 Type II, ISO 27001 or equivalent shall be accepted. CERT-In empanelled audit reports shall be applicable only to components/services for which such India-specific audit is contractually and technically feasible."	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3460	7	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	92	The application and DB is/will be hosted separately on a dedicated infrastructure (physical/logical) for PSB. Evidence of dedicated infrastructure (physical/logical) for PSB should be submitted.	The proposed platform is an OEM-managed hosted security service designed with logical access controls and customer data isolation. Requiring dedicated physical application/database infrastructure would restrict standard SaaS/POD architectures without necessarily improving the security outcome. We request acceptance of secure logical tenant/customer isolation supported by independent assurance evidence. " The proposed hosted service shall provide secure logical segregation/isolation of Bank data and administrative access from other customers through appropriate access-control and tenant-isolation mechanisms. Dedicated physical application/database infrastructure shall not be mandatory where equivalent logical isolation is implemented and independently assured."	Please refer addendum for the revised clause
3461	8	All Solution Deployed on Cloud Should Submit the compliance to these requirement respectively for each solution	98.1	Feasibility to audit/review IT controls of the third party or obtaining independent review report for the same from CERT-In empaneled security consultant, to ensure it meets Bank's information security requirement.	We request that the Bank permit review of current independent assurance reports/certifications as the primary mechanism for reviewing OEM IT controls. Any direct audit should remain subject to the OEM's standard contractual audit provisions, confidentiality, security, scope and advance-notice requirements." The Bank may review applicable independent third-party assurance reports/certifications covering the hosted service. Where additional audit is required, such audit shall be subject to mutually agreed scope, confidentiality/security restrictions, reasonable advance notice and the OEM's standard contractual audit provisions. A CERT-In empanelled consultant may review evidence made available under these conditions."	Please refer addendum for the revised clause
3462	Appendix 1A Page 40	NDR Functional Compliance Sheet	Clause 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high- availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	The Clause mandates Cloud based SaaS model, while RFP Page 30, Page 35, section 7.2.4.1 clause 'd' asks for on Premesis solution "The NDR shall be deployed On-Premises". We request to modify the clause to include On-Prem solution. Justification: To include solutions which are on-Prem based	Please refer Addendum for revised clause
3463	Appendix 1A Page 40	NDR Functional Compliance Sheet	Clause 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high- availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	The Clause asks for Active-Active HA architecture, we request to include Active-Standby Mode. Justification: Management Console is central console, it cannot be deployed in Active-Active mode, as it is a central component.	Please refer Addendum for revised clause
3464	Appendix 1A Page 41	NDR Functional Compliance Sheet	Clause 18	Solution should have the capabilities to create and run security playbooks for automation and better MTTD/MTTR on the basis of criticality of threat/server	Proposed solution adopts below appraoch for automated MTTD, Solution need investigative workflows and all the alerts need to be validated before building any Active Response Solution is having inbuilt playbooks like Host, Session and Packet analysis. once alert is validated Active Response can be triggered. Hope the approach is acceptable	Please refer addendum for the revised clause
3465	Page 66	7.6.7	Training	At a minimum, the following training programs shall be conducted for each proposed solution / OEM appointed officials: Duration per Session and Munimum Number of Sessions	Overall there is a requirement of 15 Sessions and Duration per session is 2 or 3 days. This takes the total training per solution to 40 days. This is very large reqirement of training, we request to make it to 3 days for NDR solution	Please refer addendum for revised clause
3466	Page 63	7.6.6	Testing, clause 3	The bidder shall provision and maintain dedicated Development, Testing, UAT, and Pre-Production environments throughout the contract period.	Is UAT Environment required for NDR solution also, given that NDR is a Passive and out of path solution.	Please refer addendum for revised clause
3467	30, 34	7.2.1 Deployment Model & HA (TIP) / 7.2.4.1 Deployment Pattern	Table 7.2.1 Sr. 7; Cl. 7.2.4.1(e)	"Threat Intelligence Platform (TIP) - Cloud (SaaS) + Hybrid - Bank Location: Broker/Collector/Integrator: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR" (Table 7.2.1).	Cyble's Threat Intelligence Platform (TIP) is delivered as a fully cloud-native SaaS solution, providing continuous threat-intelligence aggregation, enrichment and distribution to the Bank via API, STIX/TAXII feed and a dedicated web portal, with high availability, geographic resiliency and disaster recovery built into the SaaS platform itself - fully aligned with the SLA, RTO and RPO defined in Section 13. As the TIP's core function requires no packet-level or in-line processing within the Bank's network, Cyble can meet the Bank's continuity requirement for this solution without deploying a broker/collector component on Bank premises. We request the Bank's confirmation that this cloud-native delivery model will be accepted as fully compliant with Table 7.2.1.	Please refer addendum for the revised deployment requirement
3468	31, 35	7.2.1 Deployment Model & HA (CSPM) / 7.2.4.1 Deployment Pattern	Table 7.2.1 Sr. 11; Cl. 7.2.4.1(i)	"Cloud Security Posture Management (CSPM) - Cloud (SaaS) + Hybrid - Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR" (Table 7.2.1); "...with the required connectors, collectors, agents, enforcers and/or other supporting Bank-side components, if required, deployed at the Bank's DC and DR in N+N Active-Active configuration" (Cl. 7.2.4.1(i)).	Cyble's Cloud Security Posture Management (CSPM) module continuously assesses the Bank's cloud environments through secure, read-only, API-based/cross-account IAM-role integration, with no agent, connector or collector required on Bank premises. This lets Cyble deliver continuous, real-time cloud security posture monitoring with high availability and resilience built natively into the SaaS platform, fully meeting the Bank's SLA, RTO and RPO requirements under Section 13. This is consistent with the qualifying language "if required" already present in Cl. 7.2.4.1(i). We request the Bank's confirmation that this API-integrated, cloud-native delivery model will be accepted as compliant.	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3469	55-56	7.4.3 Attack Surface Management	Cl. 7.4.3	"Discovery of internet-facing and internal assets... The proposed solution shall provide AI-enabled Attack Surface Management (ASM) capabilities for continuous discovery... of the organization's external attack surface, including known and unknown internet-facing assets."	Cyble's Attack Surface Management (ASM) capability provides continuous, AI-enabled discovery, monitoring and risk-prioritization of the Bank's entire external attack surface - internet-facing assets, exposed services, domains, cloud assets and shadow IT - using external/passive reconnaissance together with Bank-shared asset inventories (IP ranges, domains, cloud accounts), with no agent or appliance required inside the Bank's network, consistent with the offsite Managed Service model in Section 7.2.2. This gives the Bank a complete outside-in exposure view from Day 1. We request the Bank's confirmation that this externally-led, agentless approach satisfies Cl. 7.4.3.	Bank is looking for external attack surface management
3470	55	7.4.5 Anti-Phishing	Cl. 7.4.5	"...offsite continuous anti-phishing monitoring and response services for detection, analysis for phishing attacks targeting the Bank, its employees, customers, executives, digital assets, domains, and online channels."	Cyble is fully equipped to deliver continuous, 24x7 Anti-Phishing monitoring across the Bank's domains, executives and digital channels from Day 1 of the engagement, scaling seamlessly as the Bank's digital footprint grows, with no additional infrastructure required from the Bank. To finalise the onboarding plan, we request the Bank share the number of primary/registered domains, sub-domains, executive/VIP identities and customer-facing digital channels to be covered at contract commencement, so Cyble can confirm precise sizing against this scope.	Please refer to the relevant Addendum for updated specfications
3471	57	7.4.6 Dark Web Monitoring	Cl. 7.4.6	"...offsite, tool-based continuous dark web and cyber threat exposure monitoring services... across the surface web, deep web, dark web, underground forums, messaging platforms, and data leak repositories."	Cyble's Dark Web & Cybercrime Monitoring capability continuously covers the surface web, deep web, dark web, underground forums, messaging platforms and data-leak repositories, and can begin protecting the Bank's specified identities, brand keywords and domains immediately upon contract signature. To tailor this coverage precisely, we request the Bank share the initial monitoring scope (employee/executive identities, brand keywords, domains and relevant data categories) so Cyble can confirm sizing and reporting cadence.	Details shall be shared with succesful bidder
3472	57	7.4.7 Threat Intelligence Feed	Cl. 7.4.7(l)	"Provision of threat intelligence through a centralized portal/dashboard and/or machine-readable feeds."	Cyble's Threat Intelligence Feed is delivered through both a centralized portal/dashboard and machine-readable, standards-based feeds (STIX/TAXII, MISP-compatible formats and API), enabling seamless integration with the Bank's existing or future security stack whenever required. We confirm this dual delivery model - portal-based consumption plus machine-readable feed/API - and request the Bank's confirmation that it satisfies Cl. 7.4.7.	No Change, Please be guided by the RFP
3473	57-58	7.4.8 Threat Hunting Services	Cl. 7.4.8(m)	"The threat hunting service shall be delivered remotely/offsite using secure and mutually agreed mechanisms for accessing relevant logs, telemetry, security tools, and data made available by the Bank."	Cyble can deliver proactive, intelligence-driven Threat Hunting entirely offsite - correlating curated external threat intelligence (IOCs, IOAs, TTPs, threat-actor and campaign intelligence) against Bank-shared context, supplemented by secure, mutually agreed read-only access to relevant Bank telemetry for validation and deeper investigation as needed - fully consistent with the remote/offsite delivery model mandated in Cl. 7.4.8(m). We request the Bank's confirmation that this intelligence-led hunting model, combined with agreed read-only telemetry access, meets the Bank's requirement.	No Change, Please be guided by the RFP
3474	58	7.4.9 Brand Protection and Monitoring	Cl. 7.4.9(j)	"Takedown coordination with relevant registrars, hosting providers, platforms, application stores, social media platforms, and other relevant entities, wherever applicable."	Cyble's Brand Reputation Monitoring capability continuously identifies brand impersonation, typosquatting, phishing/fraudulent websites, fraudulent mobile apps and social-media impersonation, and actively coordinates takedown requests with registrars, hosting providers, app stores and social platforms on the Bank's behalf under a standard authorisation executed at contract signature - delivering a fully managed, end-to-end takedown process with minimal effort required from the Bank's team. We request the Bank's confirmation that this bidder-led takedown coordination model satisfies Cl. 7.4.9(j).	Please refer addendum for revised clause
3475	256	16.21 Annexure 21: Sizing/Volumetrics (gap for Offsite Services)	Annexure 21, Sizing table	Annexure 21's sizing table provides explicit volumetrics (EPS, endpoint counts, IPs, VPCs, etc.) for the 14 solutions under Section 7.3, but no equivalent executive/VIP count is specified for the offsite services that monitor executive exposure (Anti-Phishing - Cl. 7.4.5, Dark Web Monitoring - Cl. 7.4.6, Brand Protection - Cl. 7.4.9).	Cyble's Executive Monitoring and Digital Risk Protection capabilities can protect any number of the Bank's executives/VIPs from Day 1, with coverage scaled precisely to the Bank's requirement across Anti-Phishing, Dark Web Monitoring and Brand Protection. To finalise sizing, we request the Bank confirm the number of executives/VIPs (e.g., Board members, CXOs, senior management) to be brought under continuous monitoring at contract commencement.	Please refer to the relevant Addendum for updated specfications
3476	256	16.21 Annexure 21: Sizing/Volumetrics (gap for Offsite Services)	Annexure 21, Sizing table	As above - no domain/sub-domain count is specified for the offsite services that monitor the Bank's external digital footprint (Attack Surface Management - Cl. 7.4.3, Anti-Phishing - Cl. 7.4.5, Brand Protection - Cl. 7.4.9).	Cyble can bring any number of the Bank's domains and sub-domains under continuous monitoring across Attack Surface Management, Anti-Phishing and Brand Protection from Day 1. To finalise sizing, we request the Bank confirm the number of primary domains and sub-domains to be monitored at contract commencement, and the expected annual growth in this count.	details shall be shared with successful bidder
3477	54	7.4 Functional Requirement - Services (Offsite Services)	Cl. 7.4(d)	"The Bidder shall implement appropriate security controls, including data masking or tokenization for sensitive data, Role-Based Access Control (RBAC), Just-in-Time (JIT) privileged access, and comprehensive audit logging for all services delivered under this RFP." - no named-user/license count is specified for platform/dashboard access to the 9 offsite services.	Cyble's platform can be provisioned for any number of the Bank's analysts, CISO-office and compliance stakeholders who need dashboard access to the offsite services, with full role-based access control as required under Cl. 7.4(d). To size the commercial bid precisely, we request the Bank confirm the number of named analyst/console user licenses required for the Bank's teams to access Cyble's platform and reporting for the proposed offsite services.	details shall be shared with successful bidder
3478	55, 58	7.4.5 Anti-Phishing / 7.4.9 Brand Protection and Monitoring	Cl. 7.4.5; Cl. 7.4.9(j)	Neither clause, nor Annexure 21, specifies an expected volume of takedown actions per month/year for phishing sites, fraudulent domains, or fake social media/mobile app listings.	Cyble is fully equipped to execute takedown actions at whatever volume the Bank's threat exposure requires. To align commercial terms precisely with the Bank's risk profile, we request the Bank confirm the estimated number of takedown actions (phishing sites, fraudulent domains, fake social media/mobile app listings) expected per month under Anti-Phishing and Brand Protection.	Please refer to the relevant Addendum

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3479	259	16.21 Annexure 21: Sizing/Volumetrics, Data Retention and Current Infrastructure	Volumetrics-Solution-wise Requirements	Proposed Solution must cover complete scope of min of 200 applications, networks, devices with 50 segments across DC-DR and capability to add additional decoy connector through decoy customization as per requirement of PSB. All the inline components of the solution must operate in high availability mode. In the event of any component failure, the system should automatically initiate failovers within seconds, ensuring uninterrupted functionality without requiring manual intervention	To ensure our proposal is accurately scoped and priced, could you please provide a comprehensive definition of the required coverage by: Confirming all in-scope network environments and segments, specifically clarifying whether the scope includes Production Data Centers (DC), Disaster Recovery (DR) sites, their associated DMZs, non-production zones (e.g., Dev, QA), and any other segments such as corporate user networks or cloud environments. Providing the approximate total number of endpoints (workstations) within these in-scope areas where deception technology (Lure & Breadcrumb) is expected to be deployed. Can we consider number 12000 Endpoint Users Scalable to 14000 as mentioned for XDR	Please refer addendum for revised clause
3480	45	APPENDIX 1A Functional Compliance Sheet (Solutions)	Decoy	Deployment capability:- • Should support auto VLAN detection and addition to deployment networks. • Should support command line based approach for Decoy deployment	1. Auto VLAN detection can be intrusive for a critical bank network. Scanning the network for VLAN is going to generate lot of traffic which may have potential impact on production network. Industry best practice is to deploy honey pot solution in the vlan selected by admins. Request the bank to make the point "Should support auto VLAN detection and addition to deployment networks." as optional 2. The proposed solution is a SaaS-based deception platform, and as is standard with cloud-hosted solutions, a native command line interface for decoy deployment is not applicable in this architecture. All deployment and management operations are delivered through a highly interactive management UI and fully documented OpenAPI-compliant REST APIs. In light of this, we respectfully request the bank to consider either: - Making this requirement optional, recognizing that modern SaaS-based deception platforms deliver equivalent or superior deployment flexibility through UI and API-based interfaces, or - Removing this requirement entirely, as mandating a CLI-based approach may inadvertently restrict the evaluation to on-premises or legacy deployment models, excluding capable cloud-native solutions from consideration. Could the bank please confirm whether this requirement can be treated as optional or waived for SaaS-based solutions?	No Change, Please be guided by the RFP
3481	45	APPENDIX 1A Functional Compliance Sheet (Solutions)	Decoy	Decoy must support Detect Malware dropped onto Decoy, categorizing any websites visited from Decoys and In-depth malware analysis against malicious code. When a threat is detected, deception should assess the event severity.	The requirement mentions "categorizing any websites visited from Decoys" however, from a security standpoint, permitting outbound internet connectivity from decoys introduces risk, as decoys are intended to be isolated environments that capture attacker behavior. Could the bank please clarify: - Is outbound internet access from decoys mandatory for compliance, or would a solution that blocks all outbound connectivity from decoys while still capturing attacker activity (commands executed, files dropped, lateral movement attempts, credential usage) be considered compliant? - If website categorization is mandatory, would it be acceptable to fulfill this through passive DNS/URL capture and offline categorization (i.e., logging the URLs/domains the attacker attempts to reach, without actually permitting the outbound connection), rather than live internet access from the decoy?	No Change, Please be guided by the RFP
3482	45	APPENDIX 1A Functional Compliance Sheet (Solutions)	Decoy	Proposed deception must support SOC integration where deception solution must allow: - ii. SOAR Solution the ability to deploy, start, stop, delete, the decoy in deception solution.	a. The proposed deception solution provides OpenAPI-compliant REST APIs that enable a SOAR platform to programmatically perform decoy lifecycle operations including start, stop, and delete. Will this be considered compliant with the stated requirement? b. The requirement also mentions "deploy" as a lifecycle action — could the bank please clarify what is meant by deploy in this context: - Does "deploy" mean provisioning a new decoy from scratch (new decoy creation/configuration), or - Does it refer to activating/starting a pre-configured decoy that already exists in the deception platform?	Yes, Bidder can achieve the requirement through any of the methods
3483	45	APPENDIX 1A Functional Compliance Sheet (Solutions)	Decoy	Eliminate External and Internal Attacks to/from decoys by identifying intrusions, malware, and website visits	a. The term "eliminate" is noted — does this mean the solution must actively block/contain attack traffic, or is detection, alerting, and integration with blocking controls (firewall/EDR) via API considered sufficient? b. For "website visits from decoys," is this referring to monitoring outbound HTTP/HTTPS traffic initiated by attacker activity on the decoy, and categorizing it for threat intelligence purposes? our solution maintains strict outbound isolation on decoys — would passive logging of attempted outbound connections satisfy this requirement?	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3484	45	APPENDIX 1A Functional Compliance Sheet (Solutions)	Decoy	The deception module generates actionable threat intelligence based on decoy interactions, with insights on attacker behaviors like botnet activity, frequent attacks, security scanner usage, and other IP attributes. Includes real-time traffic patterns (hourly, weekly, monthly) and detailed attack types (region-wise, ISP-wise, decoy-wise).	Our solution natively captures and correlates attacker behavior across all decoy interactions, including source IP, geolocation, ASN/ISP, attack type, frequency, and decoy-specific interaction details. The platform supports log forwarding and API-based export of threat intelligence to external SIEM/TIP platforms (e.g., Splunk, Microsoft Sentinel, IBM QRadar) via Syslog/CEF and REST API, where traffic pattern visualization (hourly/weekly/monthly) and custom reporting can be configured. Could the bank please confirm whether SIEM/TIP-based visualization and custom reporting via API/log forwarding is acceptable as compliant?	No Change, Please be guided by the RFP
3485	45	APPENDIX 1A Functional Compliance Sheet (Solutions)	Decoy	Includes an algorithm for automated rule creation that integrates with SOAR platforms, enabling real-time blocking of attacker IPs based on threat intelligence gathered from decoys. Features a customizable Generative AI model to assist security analysts with contextual insights, investigative support, and proactive security measures.	Our Deception solution forwards attacker IPs and threat intelligence to the SIEM in real-time, where automated rule creation and SOAR-based IP blocking are orchestrated — which is industry best practice, as SIEM acts as the centralized correlation hub across all security telemetry, not just deception events. For GenAI-assisted analyst support, leading SIEM/SOC platforms already provide this natively across all security data including deception events, offering a far richer and unified analyst experience than a standalone GenAI within a deception product. Could the bank please confirm whether SIEM-driven orchestration and SOAR-based blocking triggered by deception telemetry, and SIEM-native GenAI, are acceptable as compliant with this requirement?	Please refer addendum for revised clause
3486	45	APPENDIX 1A Functional Compliance Sheet (Solutions)	Decoy	The proposed solution shall support integration with endpoint protection, anti-malware, IPS, NGFW, EDR/XDR, SIEM, SOAR, and other enterprise security solutions to correlate deception events with endpoint, network, and security telemetry.	Our solution forwards all decoy interaction events and threat intelligence logs to external SIEM platforms (e.g., Splunk, Microsoft Sentinel, IBM QRadar) via Syslog/CEF and REST API, where correlation with endpoint, network, and security telemetry from other solutions (EDR/XDR, NGFW, IPS, SOAR etc.) can be performed. Could the bank please confirm whether SIEM-based event forwarding and correlation is acceptable as compliant with this requirement?	No Change, Please be guided by the RFP
3487	Page No.	Section	RFP Clause	Clause / Technical Specification	Bidder's Query	No Change, Please be guided by the RFP
3488	7	KEY INFORMATION	Security Deposit/Earnest Money deposit	Rs. 4.25 Crore (INR Four Crore and Twenty-Five Lakh Only) Note: - Bidders who are eligible for EMD (Earnest Money Deposit) exemption as per GeM General Terms and Conditions (GeM 4.0, Version 1.25, dated 14th July 2025, Page 19) are required to submit a Bid Security Declaration in lieu of EMD. Please refer to RFP, Annexure 4: Bid Security Declaration for the prescribed format. This declaration must be duly filled, signed, and submitted along with the bid documents by vendors seeking the waiver of EMD submission. Failure to submit the Bid Security Declaration (where applicable) will result in the bid being treated as non-responsive.	The RFP stipulates an EMD of ₹4.25 Crore and states that bidders eligible for EMD exemption as per GeM General Terms and Conditions (GeM 4.0, Version 1.25 dated 14th July 2025, Page 19) are required to submit a Bid Security Declaration in lieu of EMD. We request the Authority to kindly confirm whether bidders who are eligible for EMD exemption under the applicable GeM provisions as on the date mentioned above shall be permitted to participate in the tender without submitting the EMD of ₹4.25 Crore, subject to submission of the prescribed Bid Security Declaration as per Annexure 4 of the RFP. Further, kindly confirm that submission of the duly signed Bid Security Declaration shall be considered sufficient compliance with the EMD requirement for such eligible bidders and that their bids shall not be treated as non-responsive solely on account of non-submission of the EMD.	No Change, Please be guided by the RFP
3489	101	Eligibility Evaluation Criteria	10.2, Eligibility Evaluation Criteria	The bidder should have a minimum average turnover of INR 500 crore per annum in India during the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth. Note – In case of MSMEs only, the turnover may be relaxed subject to meeting the quality and technical speci cations.	Considering the size and EMD of the project, Turnover of 400 crore is very high. Further various guideliness of government does not recomend such restrictive clause. Hence we request the department to change this clause as The bidder should have a minimum average turnover of INR 400 crore in India during the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth. Note – In case of MSMEs only, the turnover may be relaxed subject to meeting the quality and technical speci cations.	No Change, Please be guided by the RFP
3490	136	12.4	Payment Terms	Annually in Advance: Upon submission of a Bank Guarantee equivalent to 110% of the annual subscription/Annual technical cost of the respective product, valid for the applicable subscription period; or Quarterly in Arrears	As bidder will already submit the PBG, we request PSB to kindly remove 110% BG for advance payment.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3491	110	Main section: (10.2) Eligibility Evaluation Criteria Sub section: OEM Evaluation Criteria (19)		The proposed OEM SIEM Solution with a minimum capacity of 30,000 EPS or 1.2 TB/day shall have been successfully implemented and be under management/maintenance in at least one (1) BFSI in India. and The proposed OEM SIEM Solution with a minimum capacity of 30,000 EPS or 1.2 TB/day shall have been successfully implemented on cloud in one (1) in India.	Kindly requesting to Amend or Modify the Clause as: " The proposed OEM SIEM Solution with a minimum capacity of 30,000 EPS or 1.2 TB/day shall have been successfully implemented and be under management/maintenance in at least one BFSI/ PSU/ PSE/ Government Organizations / Private sector in India" and The proposed OEM SIEM Solution or the Bidder, with a minimum capacity of 30,000 EPS or 1.2 TB/day, shall have been successfully implemented in at least one organisation in India, either in a Cloud or On-Premises deployment This will help technically qualified OEMs to come forward and participate, providing the customer with a wider choice of reliable and technically capable solutions.	Please refer addendum for revised clause.
3492	68	7.7 On-cloud proposed solution OEM Responsibilities (10)		The OEM shall have valid ISO/IEC 27001 certification and SOC 2 Type II report.	We kindly request you to remove or modify this clause: The OEM/Bidder shall have valid ISO/IEC 27001 certification and SOC 2 Type II report. SOC 2 Type II is primarily relevant to organisations responsible for hosting and managing services and provides assurance over controls related to the service environment. Making this requirement mandatory for the OEM may restrict participation of technically qualified OEMs who have proven capabilities and valid ISO/IEC 27001 certification. We assure you that our proposed solution adheres to all the essential specifications outlined in the bidding document and is well-equipped to meet the operational requirements effectively.	Please refer addendum for the revised clause
3493					Kindly requesting to confirm the delivery days to ensure smooth processing for SIEM solution	Please be guide by the RFP. Bidder to submit the detailed implementation timeline as asked in RFP
3494					Kindly confirm whether any remote locations are in scope for log collection. If yes, kindly provide the details of such locations and confirm whether these locations are interconnected with network infrastructure or require separate connectivity for log forwarding.	Details shall be shared with the successful bidder
3495	258	Main Section: 16.21 Annexure 21: Sizing/Volumetrics, Data Retention and Current Infrastructure	Sub Section:16.21.2 Volumetrics-Solution-wise Requirements: Point: (1.SIEM)	Total 50,000 sustainable EPS/ 2.06 TB per day (whichever is higher) of data ingestion from the outset scalable to Total 75,000 sustainable EPS/ 3.09 TB per day (whichever is higher) at DC & DR.	Request to kindly provide an EPS range with a clear lower and upper limit to better understand the scale of the opportunity.	Please refer addendum for the revised clause
3496	37	Main Section: 7.2.4.3 Storage and other Requirement	Sub Section: 2. For SIEM Solution Point: Primary Log Storage & Retention	.Raw SIEM logs shall be retained on the Cloud-designated primarystorage for a minimum period of 1 month in their original/unmodified form, along with relevant timestamps, source information and metadata. □ Parsed, normalized, enriched, indexed and correlated logs, together with associated metadata and contextual information, shall be retained for a minimum period of 60 months (5 years). □ The Bidder shall provision adequate storage considering ingestion volumes, growth, processing, indexing, retention and applicable overheads.	Kindly requesting you to provide the details of the online and offline log retention.Details of online and offline log retention ensures that we have a comprehensive understanding of the solution's data storage and retention capabilities, which is crucial for compliance, incident investigation, and operational planning	No Change, Please be guided by the RFP
3497	258	Main Section: 16.21 Annexure 21: Sizing/Volumetrics, Data Retention and Current Infrastructure	Sub Section:16.21.2 Volumetrics-Solution-wise Requirements: Point: (1.SIEM)	The bank will procure additional Licenses in the tranches of 10,000 EPS/ 420 Gb per day based on the rate provided in the BOM.	The RFP specifies that additional SIEM capacity may be procured in increments of 10,000 EPS / 420 GB per day. Kindly clarify whether the bidder is required to provide a unit price for each additional 10,000 EPS / 420 GB per day capacity tranche is applicable throughout the entire contract period, including any extensions,also clasify the quoted unit rate will remain fixed for future capacity augmentation.	The SIEM is being procured as a SaaS solution. Additional capacity shall be procured in 10,000 EPS / 420 GB/day tranches. The quoted rates shall include the required cloud infrastructure, storage, compute, connectivity and associated data-transfer costs as specified in the RFP.
3498		Main Section: Technical compliance - Functional Specification	Sub Section: SIEM Solution Point: 15.1	File reputation	As per the requirement for “File Reputation”, Kindly clarify whether the intended functionality refers to reputation checking of files based on file hash or File Integrity Monitoring (FIM) to detect unauthorized changes/modifications to files.	No Change, Please be guided by the RFP
3499		Main Section: Technical compliance - Functional Specification	Sub Section: SOAR Solution Point: 2	Proposed SOAR solution should have 70+ OOTB and should allow creation of 100s of playbooks. It should support OOTB integration with 100+ different OEM products. It should support more than 2500+ automated actions. It should have a bi-directional integration with SIEM solution, and can also be able to integrate with all industry leading SIEM solution. The OEM should additionally provide playbook creation, deletion, or custom integration services at no extra cost to the Bank in order to meet the rquirement stated in the RFP and Functional rquirement	The RFP requires the SOAR solution to support more than 2,500 automated actions. Kindly clarify the need for this specific number, as it may be restrictive. Kindly remove the fixed “2,500+” requirement.	No Change, Please be guided by the RFP
3500		Main Section: Technical compliance - Functional Specification	Sub Section: NDR Solution Point: 5.4	Voice: SIP, H232, RTSP, RTP, SCCP	Kindly requesting to remove the clause.	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3501		Main Section: Technical compliance - Functional Specification	Sub Section: SOAR Solution Point: 5.7	Remote Desktop: Microsoft Remote Desktop, Citrix ICA, VMWare and Citrix Channel	The RFP specifies support for Microsoft Remote Desktop, Citrix ICA, VMware, and Citrix Channel. Kindly confirm whether Citrix ICA is currently being used by the Bank. If Citrix ICA is not in use, we request the Bank to consider removing this specific requirement.	Please refer addendum for the revised clause
3502		Vulnerability Assessment & vulnerability lifecycle Management	3	The proposed solution shall be software-based and fully deployable on the hardware infrastructure proposed by the Bidder.	If SIEM, SOAR, Threat Intelligence and other solutions are permitted in a cloud-based model, why is VA-VM specifically mandated to be on-premises? This appears to be an OEM-specific clause. We have several Indian banking customers successfully using our VA solution for years. Request the Bank to kindly relax this clause and allow cloud-based VA-VM deployment.	No Change, Please be guided by the RFP
3503		Vulnerability Assessment & vulnerability lifecycle Management	10	The proposed solution shall support deployment across physical, virtual, and containerized environments.	If SIEM, SOAR, Threat Intelligence and other solutions are permitted in a cloud-based model, why is VA-VM specifically mandated to be on-premises? This appears to be an OEM-specific clause. We have several Indian banking customers successfully using our VA solution for years. Request the Bank to kindly relax this clause and allow cloud-based VA-VM deployment.	No Change, Please be guided by the RFP
3504		Vulnerability Assessment & vulnerability lifecycle Management	12	The management console shall support deployment in both Primary and Disaster Recovery (DR) sites with secure synchronization and failover capabilities.	If SIEM, SOAR, Threat Intelligence and other solutions are permitted in a cloud-based model, why is VA-VM specifically mandated to be on-premises? This appears to be an OEM-specific clause. We have several Indian banking customers successfully using our VA solution for years. Request the Bank to kindly relax this clause and allow cloud-based VA-VM deployment.	No Change, Please be guided by the RFP
3505		Vulnerability Assessment & vulnerability lifecycle Management	30	The proposed solution should provide predictive risk analysis or exploitability assessment based on vulnerability intelligence and threat context.	If SIEM, SOAR, Threat Intelligence and other solutions are permitted in a cloud-based model, why is VA-VM specifically mandated to be on-premises? This appears to be an OEM-specific clause. We have several Indian banking customers successfully using our VA solution for years. Request the Bank to kindly relax this clause and allow cloud-based VA-VM deployment.	No Change, Please be guided by the RFP
3506		Vulnerability Assessment & vulnerability lifecycle Management	33	The proposed solution shall support deployment and lifecycle management of scanning agents without dependency on cloud-hosted services.	If SIEM, SOAR, Threat Intelligence and other solutions are permitted in a cloud-based model, why is VA-VM specifically mandated to be on-premises? This appears to be an OEM-specific clause. We have several Indian banking customers successfully using our VA solution for years. Request the Bank to kindly relax this clause and allow cloud-based VA-VM deployment.	No Change, Please be guided by the RFP
3507	95, 98	Sections 7.19.2, 8 and 9		Section 7.19.2 Transition Management: 2. The Bidder shall take over and maintain the operations and support of the Bank's existing solutions with effect from 01.05.2027, on an 'as-is and where-is' basis, and shall continue to provide uninterrupted operations and support until the proposed/new solution is successfully implemented, commissioned, and goes live, in accordance with the requirements of this RFP. 3. The Bidder shall deploy the required qualified and experienced support resources at the Bank's premises with effect from 01.05.2027 to perform the day-to-day operations, monitoring, administration, troubleshooting, maintenance, incident management, and support of the existing solutions. The 'as-is and where-is' basis shall not exempt the Bidder from meeting the applicable SLAs or from any consequences arising from a breach of such SLAs. 4. The bidder shall run the existing SIEM on as-is/where-is basis for another 12 months from the date of Go-Live of the respective solutions. Section 8 Contract Period: The contract period for the project is the Implementation Period (as mentioned in Section 9;	Bank is requested to confirm the contract commencement reference and whether the transition support from 01.05.2027 falls within or outside the 65-month period. Justification: Clarity is required to size manpower, ATS/AMC and licence subscription terms correctly in the commercial bid.	The selected bidder shall ensure Go-Live of the proposed solution within the timelines specified in the RFP. In case the bidder is unable to achieve Go-Live within the stipulated timelines, the bidder shall continue to operate and support the existing/in-scope services until successful Go-Live of the proposed solution, without disruption to the Bank's services. To ensure seamless transition of services from the existing SI to the selected bidder, the selected bidder shall take over the in-scope services from 01.05.2027 and ensure uninterrupted operations and support in accordance with the RFP requirements. The bidder shall factor the transition activities, required manpower requirement

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3508	7, 20-21	Section 1 and Clause 6.10		Section 1 Key Information: Security Deposit/Earnest Money deposit: Rs. 4.25 Crore (INR Four Crore and Twenty-Five Lakh Only). Bidders who are eligible for EMD exemption as per GeM General Terms and Conditions are required to submit a Bid Security Declaration in lieu of EMD. Clause 6.10 Earnest Money Deposit (EMD): 1. The bidder shall furnish Noninterest earning Earnest Money Deposit (EMD) amount as mentioned in the Bid Schedule by way of Bank Guarantee drawn on any Scheduled Bank in India (except Cooperative Bank, RRB & Punjab & Sind Bank) in favor of Punjab & Sind Bank, payable at Delhi. 2. The same should be valid for an additional 45 days beyond bid validity period. 3. The Bank Guarantee issued by the issuing Bank on behalf of Bidder in favor of Bank shall be in paper form as well as issued under the 'Structured Financial Messaging System' (SFMS) sent to Punjab & Sind Bank, Sector 44 Branch, Gurgaon, IFSC PSIB0021509. Any bank guarantee submitted in physical mode, including EMD/bid guarantee which cannot be verifiable through SFMS will be rejected summarily.	Bank is requested to confirm whether an insurance surety bond and/or a Bid Security Declaration would be acceptable in lieu of a Bank Guarantee. Justification: A Bank Guarantee of this value blocks bidder credit lines for the entire 180-day validity plus claim period; permitting a surety bond would widen competition.	Please refer addendum for the revised clause
3509	159-160	Clause 14.5		14.5 Dispute Resolution: If any dispute, difference or claim arises between the parties hereto in connection with the validity, interpretation, implementation or alleged breach of the terms of this Agreement or anything done or omitted to be done pursuant to this Agreement, the Parties shall attempt in the first instance to resolve the same through negotiation. If no settlement to dispute(s) or difference(s) can be reached through amicable negotiation between the Parties within 30 days of such reference, the Parties shall approach the appropriate Court of Law. However, upon mutual consultation, the Parties may also have an option to refer the dispute(s) or difference(s) for settlement by Arbitration. The place of Arbitration shall be Delhi and Courts at Delhi shall have exclusive jurisdiction over the matters covered.	Bank is requested to confirm the applicable dispute resolution mechanism. Justification: The position materially affects risk pricing and the internal approvals required by bidders before submission.	No Change, Please be guided by the RFP
3510	103-105	Section 10.2, Eligibility Criterion 7		The Bidder must have successfully supplied, installed and maintained (or under maintenance) SIEM Solution of minimum 20000 EPS / 0.86 TB per day in one PSU/PSE/Government Organizations/BFSI/Telecom provider in India in last 5 years. Note: A Bidder's experience shall be considered irrespective of when the implementation was completed. Even if the implementation was completed more than five years prior to the date of publication of the RFP, such experience shall qualify only where the same Bidder that supplied, installed and implemented the SIEM Solution is also currently maintaining the same solution, or has maintained the same solution at any time during the five-year period preceding the date of publication of the RFP.	Bank is requested to confirm that SIEM deployments delivered under a managed security services (MSSP / SOC-as-a-Service) model, where the licence is held by the service provider, will be counted towards this criterion, subject to the same EPS threshold and client certification. Justification: Several large Indian banks procure SIEM as a managed service. Recognising such deployments would allow experienced SOC operators to participate without diluting the Bank's capability requirement.	Please refer addendum for revised clause.
3511	73	Section 7.12.3, Resource Type 1		Project Manager – Implementation | Onsite (Full Time) • Graduate/B.E./B.Tech/MCA with PMP/PRINCE2 or equivalent certification. • Minimum 8 years of experience. • Proven experience in managing at least two Security Solution implementations (including at least one Perimeter Security solution) in PSU/PSE/Government/BFSI/Regulatory organizations.	Bank is requested to consider substituting this with experience of implementing SOC / SIEM or NextGen SOC solutions of comparable scale. Justification: The requirement appears to relate to the Bank's separate firewall tender. SOC implementation experience is more directly relevant to the scope of this RFP.	Please refer addendum for the revised Clause.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3512	41, 258-259	Sections 7.3.1.2 and 16.21.2		Section 7.3.1.2 SIEM Data Ingestion and EPS Measurement: Each unique event/log record shall be counted only once for SIEM EPS. Internal telemetry, intermediate processing records, replicated records, correlated alerts, or downstream workflow events shall not be counted as additional SIEM source-ingestion EPS unless they are separately generated as unique records and actually ingested by the SIEM. The use of common OEM architecture or shared backend shall not be used to combine or double-count data volumes for SIEM EPS calculation. XDR (or any other solution) native telemetry shall not be treated as additional SIEM EPS where it is not separately ingested by the SIEM for SIEM processing. Annexure 21, SIEM Volumetrics: Total 50,000 sustainable EPS/2.06 TB per day (whichever is higher) of data ingestion from the outset scalable to Total 75,000 sustainable EPS/3.09 TB per day (whichever is higher) at DC & DR. Annexure 21, UEBA Volumetrics: Total 50,000 sustainable EPS/2.06 TB per day (whichever is higher) of data ingestion from the outset scalable to	Bank is requested to confirm whether UEBA ingestion is a subset of the SIEM ingestion volume or is to be licensed as a separate, independent volume. Justification: The two interpretations differ materially in licence and infrastructure cost. A common basis will ensure comparable commercial bids.	Bank has asked exclusively for UEBA solution. Bidder to design the solution accordingly
3513	141, 143	Section 13.1, Items 13-14 and Criticality Table		13. If any critical component of the supplied solution becomes non-functional, the bidder and OEM shall, within four (4) hours of incident reporting, either: (a) repair the defective component, (b) replace it with a new equivalent component, or (c) provide a standby replacement at no additional cost to the Bank. 14. If the bidder fails to restore service or provide a replacement/standby component within the stipulated four (4) hour period, the Bank may undertake or arrange remedial measures at the bidder's risk and cost, without prejudice to any other rights and remedies available under the contract. Critical / High Incident: Response Time: Within 15 minutes (24x7x365); Resolution Time: Within 45 Minutes.	Bank is requested to confirm which timeline shall govern computation of penalties, and to align the two provisions. Justification: The two provisions currently prescribe different obligations for the same event, which creates uncertainty in penalty exposure.	No Change, Please be guided by the RFP Clarification: The 45-minute Resolution Time governs penalty computation; the 4-hour timeline governs the outer limit for physical component restoration/replacement, breach of which triggers the Bank's step-in right under Point 14 (Section 13.1), in addition to (not instead of) SLA penalties already accruing from the 45-minute breach.
3514	142	Section 13.1, Item 16		If any customer-facing application, Core Banking System (CBS), regulatory application, statutory application, or other critical banking service becomes unavailable, disrupted, or degraded due to an issue attributable to the Core Firewall or Perimeter Firewall or solution(s) supplied under this RFP, and the incident is classified by the Bank as a Critical-Level Incident, the Bank may impose an additional penalty over and above the standard SLA penalties. Where such an incident remains unresolved for more than 120 minutes, an additional penalty of 0.5% of the monthly maintenance charges shall be levied for every subsequent hour or part thereof until the issue is resolved and normal services are restored.	Bank is requested to delete or restate this provision so that it applies only to components within the NextGen SOC scope. Justification: The clause appears to have been carried over from the Bank's separate IT Security Solutions & Firewall RFP.	Please refer addendum for revised clause
3515	36-37, 150	Sections 7.2.4.3 and 13.1		Section 7.2.4.3, General requirement for all cloud deployed solutions: Restoration - The solution shall support restoration and retrieval of applicable logs, security data, databases, metadata, configurations and other relevant information from the Bank's backup and archival infrastructure. Restoration shall be completed within the RTO specified in this RFP and shall not require additional software or license charges. For SIEM Solution, Backup, Recovery & DR: The Bidder/OEM shall manage the required backup at the CSP/Cloud site for SIEM availability and recovery. In addition, raw and processed/normalized SIEM logs, configurations, policies, rules, metadata and other Bank-owned SIEM data shall be backed up/transferred to the Bank's designated backup infrastructure at DC and DR in accordance with the Bank's Backup and Data Retention Policy. Disaster Recovery (DR) Instance Availability: RPO: 15 minutes; RTO: 60 minutes.	Bank is requested to confirm the applicability of RPO / RTO to the cloud service provider layer, and whether the Bank-side copy may be maintained in an archival rather than a live, immediately searchable form. Justification: Recovery objectives for SaaS platforms are governed by the OEM's published service commitments. Archival retention would substantially reduce infrastructure cost without affecting evidentiary or regulatory needs.	The bidder shall ensure that the proposed cloud/SaaS architecture and OEM/CSP commitments are capable of meeting the specified SLA, availability, uptime and cloud service continuity requirements as defined in the RFP. No additional software or licence charges shall be applicable for meeting the stated requirements.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3516	71, 93	Sections 7.9 and 7.18.5		Section 7.9 Delivery, Installation & Commissioning, Item 8: Ownership of all supplied hardware, software licenses, subscriptions, entitlements, documentation, and other assets procured under this RFP shall vest with the Bank upon successful delivery and acceptance. For perpetual software licenses, the Bank shall receive the ownership/licensing and usage rights specified in the contract. For subscription-based or SaaS solutions, the Bank shall receive the contracted subscription, service and usage entitlements for the entire contracted period. Section 7.18.5 Software, Item 1: Bidder should propose Enterprise/OEM Supported based licenses and must issue in the name of PSB. Only supported and stable version of solution can be considered for the proposed systems. The proposed solution should be the latest and stable version.	Bank is requested to confirm how this requirement is to be applied to SaaS and subscription-based components. Justification: SaaS entitlements are typically provided as a subscription for the contract term rather than as a perpetual licence. Confirmation will enable accurate structuring of the Bill of Material.	Clarification: The bidder shall clearly specify the applicable licensing model, subscription model, usage rights and entitlements for all proposed components, including perpetual, subscription, SaaS, term-based, user-based, device-based, capacity-based and any other applicable licensing models, in the Bill of Material. For SaaS/subscription-based components, the contracted subscription, service and usage entitlements shall be valid for the entire contract period. All proposed solutions/services shall be OEM-supported and comply with the applicable requirements specified in the RFP.
3517	66	Section 7.6.7		The bidder and respective OEMs shall provide comprehensive product training, knowledge transfer, and certification programs for the Bank's IT and Information Security personnel at no additional cost. All technical and product-specific training shall be delivered by OEM. The bidder shall provide certification and training for 15 bank officials, to be completed within 12 months from the Go-Live of the solution. Failure to complete the training within the stipulated period shall attract applicable Liquidated Damages (LD). At a minimum, the following training programs shall be conducted for each proposed solution/OEM appointed officials: • Beginner/Foundation Training: 2 Days, 5 Sessions • Advanced/Administrator Training: 3 Days, 5 Sessions • Backend Administration, Troubleshooting & Maintenance Training: 3 Days, 5 Sessions.	Bank is requested to confirm the total number of training sessions envisaged, and whether sessions may be consolidated across solutions and delivered in batches. Justification: Consolidation would reduce cost and Bank officials' time commitment while achieving the same coverage and competency outcome.	All technical and product-specific training shall be delivered. The bidder shall be responsible for coordinating and ensuring delivery of the prescribed training and certification programs within the stipulated timelines, at no additional cost to the Bank.
3518	142, 157-158	Sections 13.1, 13.2 and 13.3		Section 13.1, Item 18: Total penalties due Service level and liquidated damages shall not exceed 10% of the Total contract value. Section 13.2 Penalties: For the purpose of this RFP, the total penalties as per LD & SLA will be subject to a maximum of 10% of the overall contract value. Section 13.3 At-Risk Amount: The monthly At-Risk Amount (ARA) shall be 15% of the estimated monthly payout of the respective month.	Bank is requested to confirm that the 10% cap is an absolute ceiling applicable to all penalty heads, including those expressed in absolute rupee terms. Justification: An express and consolidated cap will allow bidders to provision risk accurately and price competitively.	The At-Risk Amount is a contractual performance mechanism and shall be withheld/adjusted in accordance with the applicable performance requirements specified in the RFP. It shall not automatically be treated as an additional penalty or Liquidated Damages (LD). Any withholding, adjustment or recovery under the At-Risk Amount shall be accounted for within the overall 10% penalty/LD cap specified in Section 13.2 and shall not be over and above such cap.
3519	59, 61, 64, 66, 76, 159	Sections 14.1		Section 14.1 Assignment & Subcontracting, Item 1: The selected bidder shall not subcontract/JV/Consortium or permit anyone to perform any of the work, service or other performance required under the contract (excluding Proposed OEM personnels). All bidder's personnel proposed for the bank shall be on bidder's Payroll.	Bank is requested to confirm that OEM-delivered services and OEM personnel engaged for implementation, certification and architecture assessment shall not be construed as subcontracting. Justification: Confirmation will allow bidders to comply with both requirements without risk of being held in breach.	No Change, Please be guided by the RFP
3520	45	Section 7.3.6.2		7.3.6.2 Key Deliverables: 1. The bidder should Provide a Centralized Management Console with customizable dashboard and role-based admin. 2. Restore the logs/data from backup for forensic investigation and as per bank requirement without any additional cost.	Decoy/HoneyPot technology is more about enriching the SIEM's detection capabilities, and the SOAR's enrichment for related playbooks. The requirement may be reworded as suggested. Justification: This clause shold read as Key Deliverables: 1. The Bidder shall deploy Decoy/Honeypot solutions to generate high-fidelity alerts and enrich SIEM detection capabilities by capturing attacker behavior. 2. The Bidder shall integrate Honeypot alerts with SIEM and SOAR to enable real-time enrichment, improved correlation, and automated response playbooks.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3521	75	Section 7.12.4		Minimum Resource Count Deployment: Shift A: L1 (Minimum) – 4; L2 (Minimum) – 2; L3/Project Manager (Minimum) – 1. The following table represents the minimum mandatory onsite resources deployment requirements. The bidder shall right-size and deploy any additional resources as required to meet the SLA, operational, security, and business requirements defined in the RFP. The Bidder shall factor in adequate backup and replacement resources to ensure uninterrupted availability (24x7x365) of the minimum required number of on-premises resources, including during planned leave, unplanned absence, attrition, training, or any other contingency.	1 L3 required for all 7 days Justification: 1 L3 should work for 5 working days to lead team.	No Change, Please be guided by the RFP
3522	Page 165-166	Limitation of Liability (Section 14.21)		Aggregate liability of bidder is capped at total Project Cost. Indirect, consequential, incidental losses, loss of profit, loss of business or revenue are excluded. Exceptions apply for IP infringement indemnity, gross negligence/willful misconduct, breach of confidentiality, and regulatory/statutory fines.	Current position is mostly acceptable as liability is limited to total contract value. However, we do have a concern with the wide carveouts particularly indemnity and breach of confidentiality. Justification: In our understanding these should also be subject to the cap.	No Change, Please be guided by the RFP
3523	Page 163	Indemnity (Section 14.13)		Indemnity is unilateral – only the bidder indemnifies the Bank against IP infringement, breach of RFP terms, and third-party claims. No reciprocal indemnity from Bank.	Indemnity provisions should preferably be mutual. Justification: Pls consider the clause below: The Client shall indemnify and hold harmless the Firm for any losses incurred or damages suffered due to: i)Third party claims ii)Any fraud, misrepresentation, or omission of facts by the Client or its personnel.	No Change, Please be guided by the RFP
3524	Page 162-163	Confidentiality (Section 14.12; Page 230-235, Annexure 13 – NDA)		NDA contains compelled disclosure provision (clause 4 of NDA) but no specific retention rights for the bidder. Obligations survive for 5 years post-termination for project confidentiality; PII/customer data/IPR obligations survive in perpetuity.	Advisable to incorporate a standard clause on Confidentiality including the right to retain information for legal and professional regulatory purposes. Justification: Pls consider adding the following: The Consultant shall be permitted to retain copies of such Confidential Information as it is required to retain for legal or professional regulatory purposes. Further confidentiality obligations should be for 1-2 years post the expiry of the engagement.	No Change, Please be guided by the RFP
3525	Page 166-168	Termination (Section 14.22-14.23)		Termination is not mutual – only the Bank has the right to terminate (on convenience or non-performance/default with 30-day cure period and 30-day notice). Bidder has no express termination right (e.g., for non-payment).	An exit option for the Bidder should be provided. Justification: Pls consider adding a termination clause that includes bidder's right to terminate for non-payment of fees within agreed period, with payment for services performed up to last day of notice including work-in-progress and demobilization costs.	No Change, Please be guided by the RFP
3526	Page 228, Page 109	Blacklisting / Debarment / Barred / Delisted Undertaking (Annexure 11; Section 10.2)		Bidder must submit self-certification confirming not blacklisted/debarred by Regulator/statutory body/Government/Government agency/Banks/Financial Institutions in India during last 3 years and as on date of bid submission. Non-compliance leads to disqualification.	Pls clarify if the status of the Consulting Agency "as on date of Bid submission" would suffice the requirements	No Change, Please be guided by the RFP
3527	30, 34	7.2.1 Deployment Model & HA (TIP) / 7.2.4.1 Deployment Pattern Table 7.2.1 Sr. 7; Cl. 7.2.4.1		"Threat Intelligence Platform (TIP) - Cloud (SaaS) + Hybrid - Bank Location: Broker/Collector/Integrator: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR" (Table 7.2.1).	Cyble's Threat Intelligence Platform (TIP) is delivered as a fully cloud-native SaaS solution, providing continuous threat-intelligence aggregation, enrichment and distribution to the Bank via API, STIX/TAXII feed and a dedicated web portal, with high availability, geographic resiliency and disaster recovery built into the SaaS platform itself - fully aligned with the SLA, RTO and RPO defined in Section 13. As the TIP's core function requires no packet-level or in-line processing within the Bank's network, Cyble can meet the Bank's continuity requirement for this solution without deploying a broker/collector component on Bank premises. We request the Bank's confirmation that this cloud-native delivery model will be accepted as fully compliant with Table 7.2.1. Justification: "Where the proposed Threat Intelligence Platform (TIP) is delivered as a cloud-native SaaS solution and does not require a Bank-premises broker/collector/integrator component to perform its core function, the Bidder may deliver the TIP solution as a fully cloud-native SaaS platform, with HA, geographic resiliency and DR provided within the SaaS platform in accordance with the SLA, RTO and RPO defined in Section 13, and such delivery shall be deemed fully compliant with the on-premises N+N Active-Active HA requirement specified in Table 7.2.1."	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3528	31, 35	7.2.1 Deployment Model & HA (CSPM) / 7.2.4.1 Deployment Pattern Table 7.2.1 Sr. 11; Cl. 7.2.4.1(i)		"Cloud Security Posture Management (CSPM) - Cloud (SaaS) + Hybrid - Bank location: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR" (Table 7.2.1); "...with the required connectors, collectors, agents, enforcers and/or other supporting Bank-side components, if required, deployed at the Bank's DC and DR in N+N Active-Active configuration" (Cl. 7.2.4.1(i)).	Cyble's Cloud Security Posture Management (CSPM) module continuously assesses the Bank's cloud environments through secure, read-only, API-based/cross-account IAM-role integration, with no agent, connector or collector required on Bank premises. This lets Cyble deliver continuous, real-time cloud security posture monitoring with high availability and resilience built natively into the SaaS platform, fully meeting the Bank's SLA, RTO and RPO requirements under Section 13. This is consistent with the qualifying language "if required" already present in Cl. 7.2.4.1(i). We request the Bank's confirmation that this API-integrated, cloud-native delivery model will be accepted as compliant. Justification: "Where the proposed CSPM solution operates entirely through cloud-to-cloud API/IAM-role based integration with no Bank-premises agent, connector or collector required, such delivery shall be deemed compliant with the HA requirement in Table 7.2.1 (Sr. 11), and cloud-native HA/DR provided by the SaaS platform in accordance with the SLA, RTO and RPO in Section 13 shall satisfy the Bank's requirement."	Please refer addendum for the revised clause
3529	55-56	7.4.3 Attack Surface Management Cl. 7.4.3		"Discovery of internet-facing and internal assets... The proposed solution shall provide AI-enabled Attack Surface Management (ASM) capabilities for continuous discovery... of the organization's external attack surface, including known and unknown internet-facing assets."	Cyble's Attack Surface Management (ASM) capability provides continuous, AI-enabled discovery, monitoring and risk-prioritization of the Bank's entire external attack surface - internet-facing assets, exposed services, domains, cloud assets and shadow IT - using external/passive reconnaissance together with Bank-shared asset inventories (IP ranges, domains, cloud accounts), with no agent or appliance required inside the Bank's network, consistent with the offsite Managed Service model in Section 7.2.2. This gives the Bank a complete outside-in exposure view from Day 1. We request the Bank's confirmation that this externally-led, agentless approach satisfies Cl. 7.4.3. Justification: "For Attack Surface Management, internal asset visibility shall be satisfied through external/passive reconnaissance and Bank-shared asset inventories (IP ranges, domains, cloud accounts), without requiring deployment of an agent or appliance within the Bank's internal network, consistent with the offsite Managed Service model defined in Section 7.2.2."	Bank is looking for external attak surface management
3530	55	7.4.5 Anti-Phishing Cl. 7.4.5		"...offsite continuous anti-phishing monitoring and response services for detection, analysis for phishing attacks targeting the Bank, its employees, customers, executives, digital assets, domains, and online channels."	Cyble is fully equipped to deliver continuous, 24x7 Anti-Phishing monitoring across the Bank's domains, executives and digital channels from Day 1 of the engagement, scaling seamlessly as the Bank's digital footprint grows, with no additional infrastructure required from the Bank. To finalise the onboarding plan, we request the Bank share the number of primary/registered domains, sub-domains, executive/VIP identities and customer-facing digital channels to be covered at contract commencement, so Cyble can confirm precise sizing against this scope. Justification: "The Bidder shall onboard the Bank-confirmed list of domains, sub-domains, executive/VIP identities and digital channels within [X] days of contract signature, with the right to revise the monitored inventory during the contract period as the Bank's digital footprint changes, at no additional cost up to an agreed variation threshold."	Please refer to the relevant Addendum for updated specfications
3531	57	7.4.6 Dark Web Monitoring Cl. 7.4.6		"...offsite, tool-based continuous dark web and cyber threat exposure monitoring services... across the surface web, deep web, dark web, underground forums, messaging platforms, and data leak repositories."	Cyble's Dark Web & Cybercrime Monitoring capability continuously covers the surface web, deep web, dark web, underground forums, messaging platforms and data-leak repositories, and can begin protecting the Bank's specified identities, brand keywords and domains immediately upon contract signature. To tailor this coverage precisely, we request the Bank share the initial monitoring scope (employee/executive identities, brand keywords, domains and relevant data categories) so Cyble can confirm sizing and reporting cadence. Justification: "The Bidder shall commence Dark Web Monitoring coverage for the Bank-confirmed scope (identities, brand keywords, domains and data categories) within [X] days of contract signature, and shall accommodate reasonable additions to this scope during the contract period as part of the Managed Service."	Details shall be shared with succesful bidder
3532	57	7.4.7 Threat Intelligence Feed Cl. 7.4.7(l)		"Provision of threat intelligence through a centralized portal/dashboard and/or machine-readable feeds."	Cyble's Threat Intelligence Feed is delivered through both a centralized portal/dashboard and machine-readable, standards-based feeds (STIX/TAXII, MISP-compatible formats and API), enabling seamless integration with the Bank's existing or future security stack whenever required. We confirm this dual delivery model - portal-based consumption plus machine-readable feed/API - and request the Bank's confirmation that it satisfies Cl. 7.4.7. Justification: "The Threat Intelligence Feed shall be delivered through the Bidder's dashboard/portal and, in parallel, as a machine-readable feed (STIX/TAXII, MISP-compatible format or API) for integration with the Bank's security tooling, and this dual delivery model shall be deemed fully compliant with Cl. 7.4.7."	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3533	57-58	7.4.8 Threat Hunting Services Cl. 7.4.8(m)		"The threat hunting service shall be delivered remotely/offsite using secure and mutually agreed mechanisms for accessing relevant logs, telemetry, security tools, and data made available by the Bank."	Cyble can deliver proactive, intelligence-driven Threat Hunting entirely offsite - correlating curated external threat intelligence (IOCs, IOAs, TTPs, threat-actor and campaign intelligence) against Bank-shared context, supplemented by secure, mutually agreed read-only access to relevant Bank telemetry for validation and deeper investigation as needed - fully consistent with the remote/offsite delivery model mandated in Cl. 7.4.8(m). We request the Bank's confirmation that this intelligence-led hunting model, combined with agreed read-only telemetry access, meets the Bank's requirement. Justification: "Threat Hunting Services shall be delivered offsite through intelligence-led investigation supplemented by secure, mutually agreed and, where necessary, read-only access to the Bank's relevant logs, telemetry and security tools, and such delivery model shall be deemed fully compliant with Cl. 7.4.8."	No Change, Please be guided by the RFP
3534	58	7.4.9 Brand Protection and Monitoring Cl. 7.4.9(j)		"Takedown coordination with relevant registrars, hosting providers, platforms, application stores, social media platforms, and other relevant entities, wherever applicable."	Cyble's Brand Reputation Monitoring capability continuously identifies brand impersonation, typosquatting, phishing/fraudulent websites, fraudulent mobile apps and social-media impersonation, and actively coordinates takedown requests with registrars, hosting providers, app stores and social platforms on the Bank's behalf under a standard authorisation executed at contract signature - delivering a fully managed, end-to-end takedown process with minimal effort required from the Bank's team. We request the Bank's confirmation that this bidder-led takedown coordination model satisfies Cl. 7.4.9(j). Justification: "The Bidder shall independently initiate and pursue takedown requests with registrars, hosting providers, platforms, application stores and social media platforms on the Bank's behalf, under a standard authorisation/power-of-attorney to be executed at contract signature, with the Bank's legal counsel engaged only in exceptional or contested cases."	Please refer addendum for revised clause
3535	256	16.21 Annexure 21: Sizing/Volumetrics (gap for Offsite Services) Annexure 21, Sizing table		Annexure 21's sizing table provides explicit volumetrics (EPS, endpoint counts, IPs, VPCs, etc.) for the 14 solutions under Section 7.3, but no equivalent executive/VIP count is specified for the offsite services that monitor executive exposure (Anti-Phishing - Cl. 7.4.5, Dark Web Monitoring - Cl. 7.4.6, Brand Protection - Cl. 7.4.9).	Cyble's Executive Monitoring and Digital Risk Protection capabilities can protect any number of the Bank's executives/VIPs from Day 1, with coverage scaled precisely to the Bank's requirement across Anti-Phishing, Dark Web Monitoring and Brand Protection. To finalise sizing, we request the Bank confirm the number of executives/VIPs (e.g., Board members, CXOs, senior management) to be brought under continuous monitoring at contract commencement. Justification: "The Bidder shall provide continuous executive/VIP monitoring for up to [N] designated executives across the Anti-Phishing, Dark Web Monitoring and Brand Protection services, with the Bank entitled to revise this list from time to time; monitoring of additional executives beyond [N] shall be chargeable at the rates quoted in the commercial bid."	Please refer to the relevant Addendum for updated specfications
3536	256	16.21 Annexure 21: Sizing/Volumetrics (gap for Offsite Services) Annexure 21, Sizing table		As above - no domain/sub-domain count is specified for the offsite services that monitor the Bank's external digital footprint (Attack Surface Management - Cl. 7.4.3, Anti-Phishing - Cl. 7.4.5, Brand Protection - Cl. 7.4.9).	Cyble can bring any number of the Bank's domains and sub-domains under continuous monitoring across Attack Surface Management, Anti-Phishing and Brand Protection from Day 1. To finalise sizing, we request the Bank confirm the number of primary domains and sub-domains to be monitored at contract commencement, and the expected annual growth in this count. Justification: "The Bidder shall monitor up to [N] primary domains and [M] sub-domains under the offsite services, with the right to revise this inventory during the contract period; monitoring of domains/sub-domains beyond the agreed baseline shall be chargeable at the rates quoted in the commercial bid."	Please refer addendum for revised clause
3537	54	7.4 Functional Requirement - Services (Offsite Services) Cl. 7.4(d)		"The Bidder shall implement appropriate security controls, including data masking or tokenization for sensitive data, Role-Based Access Control (RBAC), Just-in-Time (JIT) privileged access, and comprehensive audit logging for all services delivered under this RFP." - no named-user/license count is specified for platform/dashboard access to the 9 offsite services.	Cyble's platform can be provisioned for any number of the Bank's analysts, CISO-office and compliance stakeholders who need dashboard access to the offsite services, with full role-based access control as required under Cl. 7.4(d). To size the commercial bid precisely, we request the Bank confirm the number of named analyst/console user licenses required for the Bank's teams to access Cyble's platform and reporting for the proposed offsite services. Justification: "The Bidder shall provide [N] named analyst/console user licenses with role-based access to the offsite services' dashboards and reporting, with the Bank entitled to add further named users during the contract period at the rates quoted in the commercial bid."	details shall be shared with successful bidder

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3538	55, 58	7.4.5 Anti-Phishing / 7.4.9 Brand Protection and Monitoring Cl. 7.4.5; Cl. 7.4.9(j)		Neither clause, nor Annexure 21, specifies an expected volume of takedown actions per month/year for phishing sites, fraudulent domains, or fake social media/mobile app listings.	Cyble is fully equipped to execute takedown actions at whatever volume the Bank's threat exposure requires. To align commercial terms precisely with the Bank's risk profile, we request the Bank confirm the estimated number of takedown actions (phishing sites, fraudulent domains, fake social media/mobile app listings) expected per month under Anti-Phishing and Brand Protection. Justification: "The Bidder shall execute up to [N] takedown actions per month at no additional cost as part of the Managed Service fee; takedown volumes beyond this threshold in any month shall be chargeable at the rates quoted in the commercial bid, or the Bidder may alternatively propose an unlimited-takedown model at the Bank's option."	Please refer to the relevant Addendum
3539	29	Annexure 21 HA table (p.29) read with 7.2.4.1(c) (p.35)		XDR — deployment mode Cloud (SaaS) + Hybrid, with 'Management Console: Deployed at both Primary and Secondary sites'.	For Cloud/SaaS delivered solutions, the Bank is requested to confirm that 'Management Console deployed at both Primary and Secondary sites' means the console is accessible and fully operable from both the DC and the DR site, with platform-side high availability provided in accordance with the Section 13 SLA, RTO and RPO — rather than a customer-hosted console instance physically deployed at each site. Justification: A SaaS console is a single regional console with platform high availability. A physically deployed console at both sites is only possible under a self-hosted model, which the same RFP prohibits for XDR under clause 7.2.4.1(c). The two clauses are mutually exclusive as written.	Please refer addendum for the revised clause
3540	257258	Annexure 21, 16.21.1 and 16.21.2		16.21.2 states 'XDR solution for 12,000 users scalable to 14,000'. 16.21.1 separately lists 2,500 servers and 300 databases, alongside 12,000 branch desktops.	The Bank is requested to confirm whether the XDR quantity of 12,000 covers desktops only, or whether the 2,500 servers listed at 16.21.1 are also to be covered within that count. If servers are in scope, the Bank is requested to confirm the split between desktop and server quantities so that both can be quoted correctly. Justification: Section 7.3.4 states XDR coverage 'across endpoints and servers'. If servers are deemed in scope after award, the bid is 2,500 licences short at a different unit price, with no mechanism to re-price. This is the largest commercial exposure on the XDR line.	Please refer addendum for revised clause.
3541		Section 3, clause 6 and clause 11		All Bank data shall reside within India. No Bank data shall be transmitted, replicated, processed, accessed, stored or exchanged outside India without prior written approval from the Bank and applicable regulatory permissions.	The Bank is requested to confirm that OEM technical support and engineering access to Bank data, performed under a documented, logged and auditable process and subject to the Bank's prior written approval as already contemplated in the clause, satisfies this requirement — with all storage and processing remaining within the India region. Justification: Storage and processing within India is achievable. The clause additionally restricts ACCESS, and global OEM support operates on a follow-the-sun basis. Without this clarification the clause cannot be answered 'Complied' truthfully, and Section 15.1 forbids a conditional answer.	No Change, Please be guided by the RFP
3542	261	Section 7.2.4, Cloud/SaaS table (p.37); Annexure 21, 16.21.3		All Bank-owned data including logs, configurations, policies, rules, reports and metadata shall be backed up / transferred to the Bank's backup infrastructure at DC and DR, with monthly full backups retained in Long-Term Storage for the entire contract duration.	The Bank is requested to confirm whether the endpoint telemetry to be transferred to Bank infrastructure may be scoped to a defined security-relevant subset agreed during implementation and documented in the SOP, rather than the complete raw telemetry stream. Bidders would appreciate an indicative Bank position so that Long-Term Storage can be sized correctly at bid stage. Justification: Unfiltered endpoint telemetry for the proposed estate is of the order of hundreds of GB per day compressed, which over a five-year retention obligation becomes a very large and expensive Bank-side storage requirement. Scoping this at bid stage protects both the Bank's cost and the Bidder's sizing.	No Change, Please be guided by the RFP
3543	258259	Annexure 21, 16.21.2		'Each node/environment must be individually provisioned for full peak load' and 'all inline components must operate in high availability mode with automatic failover within seconds'.	For Cloud/SaaS delivered solutions, the Bank is requested to confirm that these requirements apply to the Bank-side components deployed at DC and DR, and that the SaaS platform's availability and capacity are governed by the service levels, RTO and RPO specified in Section 13. Justification: Node-level provisioning commitments cannot be made against multi-tenant SaaS infrastructure. Without this clarification the OEM would be signing an obligation it does not control.	Please refer addendum for the revised clause
3544		Section 3, clause 12		Bank data shall not be used for model training, retraining, analytics, or shared with third parties, whatsoever, except as explicitly authorised by the Bank in writing.	The Bank is requested to confirm whether this restriction is intended to preclude the use of anonymised and aggregated threat indicators for the purpose of improving threat detection efficacy for the Bank's own environment, or whether it is intended to apply without exception. Justification: Determines whether any AI-assisted or threat-intelligence-derived capability can be offered at all, and shapes the OEM's Data Processing Addendum position. Must be settled before the Annexure 18 declaration is signed.	The restriction shall apply without exception unless expressly authorised by the Bank in writing. Bank data, including security telemetry, logs, events, alerts, metadata, threat indicators, and other information generated from or relating to the Bank's environment, shall not be used by the Bidder/OEM for model training, retraining, product improvement, analytics, benchmarking, or any other purpose, nor shared with any third party, unless specifically authorised by the Bank in writing.

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3545	210, 211 169	Eligibility criteria #24 and #25; Section 15.1		Minimum 85% functional compliance per solution against Appendix 1A, with exceptions, disclaimers, limitations and conditional compliance not taken on record.	The Bank is requested to confirm whether a response of 'Complied through an additional licensed module included in the commercial offer' is treated as Complied for functional compliance scoring purposes, given that the module concerned is being quoted and supplied as part of the proposal. Justification: Several capabilities are delivered through licensed add-ons that are being priced in the BOQ. Confirming this treatment prevents a technically compliant, fully priced solution being marked down for describing how a capability is licensed.	The compliance of 85% should be met by each of the OEM for their respective Solution & Services as per the eligibility criteria defined.
3546	210211	Eligibility criteria #24 and #25		Compliance confirmation and 85% functional compliance are required for each of 14 listed solutions and 9 listed services.	The Bank is requested to confirm that bids comprising multiple OEMs across the listed solutions are permitted, with each OEM providing the Annexure 18 declaration and Appendix 1A compliance for the solutions it supplies. Justification: No single OEM supplies all 14 solutions and 9 services. Confirming the multi-OEM position protects the bid structure.	The compliance of 85% should be met by each of the OEM for their respective Solution & Services as per the eligibility criteria defined.
3547	39–40	7.3.1 – Security Information and Event Management 7.3.1.1, Clauses 5–6		SIEM shall integrate with the Bank's entire IT ecosystem and collect logs/telemetry from servers, endpoints, network devices, security appliances, databases, applications, access management, cloud, SaaS/PaaS/IaaS, containers, APIs and third-party systems.	Please provide the list of major data source types to be integrated with SIEM/UEBA, together with the approximate count of instances/devices for each source type.	ITSM - Manage Engine
3548	26, 34–35	7.1 / 7.2.4 – Scope & Deployment Architecture 7.1; 7.2.4.1		The solution shall cover the Bank's DC, DR, cloud environments and branches, using a hybrid model with Cloud/SaaS and Bank-hosted components.	Please share the Bank's current cloud footprint (AWS/Azure/GCP/other), key cloud services in use, and the expected cloud expansion roadmap during the contract period.	Details shall be shared with successful bidder
3549	34–36	7.2.4 – Deployment Architecture 7.2.4 / 7.2.4.2		Bank-hosted collectors/brokers/sensors/connectors shall exchange telemetry securely with Cloud/SaaS platforms across DC, DR, branches and cloud environments.	Please clarify how the in-scope data sources are distributed across DC, DR, branches, cloud accounts/subscriptions, regions and other locations, including any major network segmentation or restricted connectivity zones.	Details shall be discussed with succesfull bidder
3550	26, 28, 67	7.1 / 7.6.8 – Compliance & Security Requirements 7.1; 7.6.8, Clause 5		The proposed solution shall support compliance with RBI, CERT-In, DPDP Act, Government of India requirements, Bank policies and other applicable regulations/standards.	Please confirm the compliance and regulatory frameworks that must be specifically addressed through SIEM, UEBA, SOAR and TIP reporting/use cases, including any Bank-specific policies or audit requirements.	No Change, Please be guided by the RFP
3551	36	7.2.4.2 – Connectivity and Data Flow 7.2.4.2		Telemetry sources include users, endpoints, servers, applications, databases, network devices, IoT/OT systems, cloud services and other sources.	Please confirm whether OT/ICS telemetry is in scope. If yes, please share the OT security platform(s) currently deployed (e.g., Claroty, Nozomi), approximate number of OT assets, and whether OT and IT environments are located in the same or separate network/DC zones.	No Change, Please be guided by the RFP, further details shall be shared with the successful bidder
3552	42	7.3.2 – SOAR 7.3.2.2, Clause 2		SOAR shall integrate with SIEM, XDR, NDR, UEBA, TIP, ITSM, IAM/PAM, network, endpoint, cloud and other relevant security solutions.	Please confirm the ITSM platform to be integrated for automated ticket/case creation and updates (e.g., ServiceNow, BMC, Jira, ManageEngine), including any specific workflow or bi-directional integration requirements.	ITSM - Manage Engine
3553	42	7.3.2 – SOAR 7.3.2.2, Clauses 2–4		SOAR requires integrations and development/customization of response workflows/playbooks for enrichment, investigation, containment, remediation and response verification.	Please provide the list of security and IT technologies that are expected to be integrated with SOAR for automated enrichment and response actions.	Details shall be shared with successful bidder
3554	45–46	7.3.7 – Threat Intelligence Platform 7.3.7.1, Clauses 3–10		TIP shall aggregate, normalize, score, contextualize and manage threat intelligence from multiple sources and use validated intelligence in automation/response workflows.	Please confirm whether the Bank currently subscribes to any commercial or sector-specific threat intelligence feeds that must be integrated with TIP/SOAR. If yes, please provide the feed/provider names and integration method, where available.	Details shall be shared with successful bidder
3555	42	7.3.2 – SOAR 7.3.2.2, Clauses 3–4		The bidder shall develop, customize, test, tune and maintain response workflows/playbooks, including automated enrichment, investigation, containment and remediation.	Please share the top five priority SOAR playbooks/use cases expected to be implemented during the initial phase, along with any mandatory approval/exception controls.	No Change, Please be guided by the RFP
3556	46	7.3.7 – Threat Intelligence Platform 7.3.7.1 / 7.3.7.2		TIP shall collect intelligence from multiple sources and support IOC/IOA/TTP lifecycle management, scoring, enrichment, curation and dissemination.	Please provide the list of existing commercial, open-source, government/CERT-In, ISAC or other threat intelligence feeds/sources that are expected to be integrated with the proposed TIP.	Details shall be shared with successful bidder
3557	43	7.3.3 – UEBA 7.3.3 / 7.3.3.2, Clauses 2–3		UEBA shall continuously monitor users/entities, build behavioural baselines, and configure peer groups, trusted entities and behavioural-analysis parameters.	Please identify the authoritative identity and context sources available for UEBA onboarding (e.g., Active Directory, HRMS, IAM/IGA, PAM, VPN, EDR, DLP, email, physical access), and confirm which source should be treated as the master source for user attributes.	Details shall be discussed with succesfull bidder
3558	43	7.3.3 – UEBA 7.3.3.2, Clause 3		Configured peer groups, trusted entities and relevant behavioural-analysis parameters are required deliverables.	Please confirm the expected peer-grouping dimensions for UEBA (e.g., department, role, designation, branch/location, privileged-user status, employment type) and whether the Bank can provide these attributes from HR/identity systems.	Details shall be discussed with succesfull bidder
3559	43	7.3.3 – UEBA 7.3.3.2, Clause 9		Configured automated response workflows are required for approved high-risk behavioural alerts.	Please identify the UEBA-driven response actions that the Bank expects to automate (e.g., disable account, force password reset, revoke session, isolate endpoint, block IP) and specify which actions require analyst/manager approval.	Details shall be discussed with succesfull bidder
3560	46	7.3.7 – Threat Intelligence Platform 7.3.7.1, Clauses 8–10		The TIP shall support IOC lifecycle management, including creation, validation, enrichment, scoring, distribution, updating and expiration, along with configurable expiry periods and intelligence lifecycle workflows.	Please confirm the expected downstream systems to which curated IOCs/IOAs/TTPs are to be disseminated from the TIP (e.g., SIEM, SOAR, EDR/XDR, firewalls, proxy, email security, NDR), and whether automated push/block actions are expected or only intelligence sharing/enrichment.	Details shall be discussed with succesfull bidder
3561	57	Threat Intelligence Platform (TIP) – General, Clause 4		The solution should integrate up to multiple sources of threat intelligence required by the organization into a single management platform without any extra cost. The sources should either be part of the Intelligence Channels, or Commercial sources that the client is subscribed to.	Kindly clarify whether "without any extra cost" refers to the integration/connectors only, while subscription/license charges for separately procured commercial CTI sources will be borne/provided by the Bank, or whether the bidder is expected to include all third-party CTI subscription costs within the TIP pricing.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3562	57	Threat Intelligence Platform (TIP) – General, Clause 10		TIP Solution should have an out-of-the-box Threat Intelligence Playbook library OR integration with a third-party solution; in case a third-party solution is required, bidder shall provide the same along with integration at no additional cost.	Kindly clarify whether integration with the Bank's proposed/existing SOAR platform for implementation of the required Threat Intelligence Playbooks will be acceptable, or whether the bidder is expected to provide a separate third-party playbook platform along with the TIP.	No Change, Please be guided by the RFP
3563	57	Threat Intelligence Platform (TIP) – IOC, Clause 11.1–11.19		Solution should support reliable, actionable feeds for IP, domains, hashes, emails, file names, blacklists, malware indicators, ASN, mutex, Windows Registry Key, port, HTTP Session Object, User-Agent and associated IOC elements.	Kindly clarify whether all listed IOC types are required to be natively supported by the proposed TIP, or whether support through integrated/enrichment sources or APIs will also be considered compliant.	No Change, Please be guided by the RFP
3564	58	Threat Intelligence Platform (TIP) – Data Ingest, Clause 14		The solution should offer a wide range of commercial CTI providers out of the box, including atomic IOCs, threat bulletins and other threat intelligence offered by each provider.	Kindly clarify whether the Bank will separately provide/procure the required commercial CTI subscriptions and API credentials, or whether the bidder is expected to include the subscription cost of such third-party providers in the proposed TIP solution.	No Change, Please be guided by the RFP
3565	58	Threat Intelligence Platform (TIP) – Analytics, Clause 20		Run enrichment tools on an IOC to gain further context. The client should create user accounts on the Enrichment Sources and activate them.	Kindly confirm that licenses/subscriptions for separately procured third-party enrichment sources will be provided by the Bank, with the TIP providing the required integration and consumption capability.	No Change, Please be guided by the RFP
3566	58	Threat Intelligence Platform (TIP) – Analytics, Clause 24		The solution should enable strategic matching leading to find associated indicators that have impacted the environment. The detection should be retrospective and allows the analyst to search back in seconds without going back to the SIEM solution or any other tool. The retention is bounded to the POV period.	Kindly clarify the intended definition and duration of the "POV period" and the minimum historical retention period expected for retrospective searches.	No Change, Please be guided by the RFP. POV Period is data-retention period
3567	58	Threat Intelligence Platform (TIP) – Analytics, Clause 29		The solution should be able to answer questions related to Threat Intelligence using closed-circuit AI and it shouldn't search the web for answers.	Kindly clarify whether the Bank requires the AI processing/model to operate entirely within a Bank-controlled environment, or whether a vendor-hosted private/isolated AI capability within the approved cloud environment will be acceptable, provided that Bank data is not used for external model training or processing.	The AI capability may be vendor-hosted within the Proposed SaaS environment, provided it operates in a closed/isolated manner and Bank data is not shared with external/public AI services.
3568	58	Threat Intelligence Platform (TIP) – Integration, Clause 35		The solution should include applications to integrate and automatically manage a data feed from the solution to the security systems that the organisation requires. For POV purposes the SIEM solution will be integrated.	Kindly confirm whether standard integration mechanisms such as REST API, STIX/TAXII, webhook or equivalent supported interfaces will be acceptable for the required SIEM integration, and whether the Bank will provide the necessary SIEM API/connectivity details during implementation.	No Change, Please be guided by the RFP
3569	3	Cloud Deployment, Clause 9		OEM shall remain solely responsible for patching, infrastructure operations, logging, interoperability, API security, portability and migration support irrespective of backend infrastructure ownership.	Kindly clarify the responsibility matrix between the TIP OEM, bidder and CSP for infrastructure-level controls and operations, particularly for patching, infrastructure operations, logging, API security, interoperability and migration where the underlying cloud infrastructure is managed by the CSP.	No Change, Please be guided by the RFP
3570	4	Cloud Deployment, Clause 27		Resource pooling/Multi-tenancy: logical separation between each consumer's computing resources and network; bidder should provide details on segregation and protection of Bank data from other customers.	Kindly confirm whether a logically isolated tenant with dedicated application/database resources and appropriate security controls within a multi-tenant CSP environment will satisfy this requirement, or whether dedicated physical infrastructure is mandatory.	Logical tenancy is acceptable, provided that the proposed bidder/OEM ensure clear separation and isolation of the Bank's data, security telemetry, logs, alerts, configurations, policies, analytics, investigation data and other Bank-related information from those of other tenants. The proposed environment for bank are protected against confidentiality and integrity risks and co-mingling of data and bidder/OEM implement adequate safeguards against combining of information, documents, records and assets.
3571	5	Cloud Deployment, Clause 38		In case of completion/termination of contract, bidder shall shift the data back to Bank or designated third-party on-premises/cloud infrastructure and sort out operability issues.	Kindly clarify the expected data format and scope for reverse data migration, including historical threat intelligence, cases/investigations, configurations, dashboards, reports, audit logs and associated metadata, and whether standard export formats such as STIX, CSV or equivalent will be acceptable.	No Change, Please be guided by the RFP
3572	6	Cloud Deployment, Clause 46.5–46.7		Remote access by administrators/privileged users over Internet shall not be permitted; solution provider/CSP/cloud management team should not have access to Bank application data.	For a managed cloud-based TIP, kindly clarify the approved mechanism for OEM support, troubleshooting, upgrades and administration, particularly where vendor technical support requires controlled access to the platform.	No Change, Please be guided by the RFP
3573	7	Cloud Deployment, Clause 90		Solution provider should have captive SOC or Managed Service SOC for monitoring their systems and operations.	Kindly clarify whether monitoring by the OEM's existing 24x7 security operations/SOC for the hosted TIP service will satisfy this requirement, or whether a dedicated SOC instance exclusively for PSB is expected.	No Change, Please be guided by the RFP
3574	8	Cloud Deployment, Clause 92		Application and DB is/will be hosted separately on a dedicated infrastructure (physical/logical) for PSB. Evidence of dedicated infrastructure should be submitted.	Kindly clarify whether dedicated logical application and database resources within an isolated cloud tenant will be considered sufficient evidence of dedicated infrastructure, or whether separate physical infrastructure is required.	Logical tenancy is acceptable, provided that the proposed bidder/OEM ensure clear separation and isolation of the Bank's data, security telemetry, logs, alerts, configurations, policies, analytics, investigation data and other Bank-related information from those of other tenants. The proposed environment for bank are protected against confidentiality and integrity risks and co-mingling of data and bidder/OEM implement adequate safeguards against combining of information, documents, records and assets.
3575	10	Platform and Solution, Clause 112		Bidder shall deploy the solution in dedicated cloud instance procured in the name of Bank for hosting the application.	Kindly clarify whether the dedicated cloud instance is required to be contractually owned/procured directly by PSB, or whether a dedicated instance provisioned and operated by the bidder/OEM on an approved MeitY-empanelled CSP will be acceptable.	No Change, Please be guided by the RFP
3576	10	Scalability & Performance, Clause 122		Capability to handle sub second response time.	Kindly clarify the transaction/search scenario and workload conditions against which the sub-second response time is to be measured, including expected concurrent users, data volume and query type.	No Change, Please be guided by the RFP
3577	10	Security, Clause 138–140		Solution should support replication between primary and secondary site with RPO/RTO; replication in both directions; real-time replication and manual/automatic application shift.	For a managed SaaS/cloud-based TIP, kindly clarify whether the OEM's native high-availability/DR architecture provided through the approved CSP will satisfy these requirements, and kindly provide the expected RPO/RTO values to be considered for sizing and commercial estimation.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3578	11	Cloud Tenant, Clause 163		Solution should be deployed on dedicated cloud instance for Bank; bidder shall finalize cloud solution requirements based on volume, response time, replication and backup requirements.	Kindly confirm the expected sizing parameters for the TIP, including number of users, expected IOC/feed volume, API transactions, data retention period, storage requirement and expected concurrent users, so that the bidder can accurately size the proposed cloud instance.	No Change, Please be guided by the RFP
3579	11	Cloud Tenant, Clause 165		Solution provider shall ensure storage of data in secured environment for period defined by Bank and remove data from all environments after discontinuation.	Kindly clarify the Bank's required retention period for TIP data and whether the retention requirement applies to all historical threat intelligence collected by the platform or only PSB-specific data, investigations and generated intelligence.	No Change, Please be guided by the RFP
3580	11	Cloud Tenant, Clause 174		Solution provider should support backups on immutable storage with ransomware protection.	Kindly clarify whether immutable backup storage with ransomware protection is expected to be provided by the TIP OEM, CSP or Bank's existing backup infrastructure, and whether the associated infrastructure, storage and licensing costs are to be included in the TIP commercial quote.	No Change, Please be guided by the RFP
3581	129	Bidder's Scoring Criteria	10.3 Technical Evalutation Criteria S.No. 1 of Table		We understand that experience of solutions can be shown in single /multiple Clients/ work orders meeting the criteria. Please confirm. Also please confirm whether solutions of Identity and Access Management will qualify for Identity Threat Detection and Response.	a) Yes. Where a single OEM platform natively provides multiple solution categories, the same credentials may be considered for each applicable category, provided the submitted documents clearly establish the required scope for each category. b) No Change, Please be guided by the RFP
3582	7	Key Information Table	Performance Bank Guarantee		**BEL is a Central PSU under Ministry of Defence so we request you to accept Indemnity bond in place of Bank Guarantee towards PBG.**	Please refer addendum for revised clause
3583	29	7.2.1	Security Information and Event Management (SIEM)	Bank Location: Broker/Aggregator/Collector: HA, N+N, Active-Active at DC and HA, N+N, Active-Active at DR. Cloud (SaaS): HA Deployment aligned with the SLA, RTO & RPO (Refer Section 13). Management Console: Deployed at both Primary and Secondary sites	In the RFP, there is an ask for management console deployment across DC-DR. If the bidder is offering SAAS platform can this requirement be relaxed.	No Change, Please be guided by the RFP
3584	37	2	For SIEM Solution	Primary Log Storage & Retention (Raw SIEM logs shall be retained on the Cloud-designated primary storage for a minimum period of 1 month in their original/unmodified form, along with relevant timestamps, source information and metadata. Parsed, normalized, enriched, indexed and correlated logs, together with associated metadata and contextual information, shall be retained for a minimum period of 60 months (5 years).)	To meet this requirement can the OEM store the same in their cloud or is it expected to have the log storage done in Banks premises.	No Change, Please be guided by the RFP
3585	57	7.4.6	Dark Web Monitoring	The Bidder shall provide offsite, tool-based continuous dark web and cyber threat exposure monitoring services to identify potential exposure of the Bank's sensitive information across the surface web, deep web, dark web, underground forums, messaging platforms, and data leak repositories.	For the darkweb monitoring can you help with the domains to be considered and no of takedowns to consider in the proposal	Detailed domain and identity information shall be provided to the selected bidder on a need-to-know basis
3586	64	7.6.6	Testing- Activities are to be performed by Respective solution OEM (supported by bidder)	The Bidder shall provide offsite, tool-based continuous dark web and cyber threat exposure monitoring services to identify potential exposure of the Bank's sensitive information across the surface web, deep web, dark web, underground forums, messaging platforms, and data leak repositories.	Can this be hosted in the OEM's cloud or is it required to be hosted in banks premises?	No Change, Please be guided by the RFP
3587	68	7.7	The proposed Cloud/SaaS solution shall support Bring Your Own Key (BYOK) and/or Customer-Managed Encryption Key (CMEK) capability, enabling the Bank to maintain control over the cryptographic keys used to protect its security data		Can this clause be relaxed or read as dedicated key for the customer to be provisioned with customer security policies enforced for the same?	No Change, Please be guided by the RFP
3588	73	7.12.3	2 OEM Implementation Resources	Onsite (Full Time) OEM shall submit a detailed resource deployment plan commencement of requirement gathering. Any replacement or modification shall require prior Bank approval.	Can this clause be relaxed or read as OEM resources to be available during the deployment phase only and be made available when needed?	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3589	TQ		16.5 Annexure 5: Pre-Qualification Criteria	The Bidder must have successfully supplied, installed and maintained (or under maintenance) SIEM Solution of minimum 20000 EPS / 0.86 TB per day in one PSU/ PSE/ Government Organizations / BFSI/Telecom provider in India in last 5 years Bidder to Submit the following 3 Documents: Document 1: Copy of Purchase Order / Work Order / Contract The submitted client-issued document shall clearly indicate, either directly or through a combination of documents forming part of the same contract: a. Name of the Client. b. Date of Issue/Signing. c. Scope of Work demonstrating supply, installation and	As PO's and contract are under NDA, we request to allow customer letter as reference for qualification of reference	Please refer addendum for revised clause.
3590	TQ		10.3 Technical Evaluation Criteria	Bidder should have supplied, installed and maintained (or under maintenance) the below solutions in any one PSU/PSE/ Government Organizations / BFSI/Telecom provider in India 1. SOAR 2. UEBA 3. Extended Detection & response (XDR)/ Endpoint Detection & response (EDR) 4. Network Detection & response (NDR) 5. Threat Intelligence Platform 6. Vulnerability Assessment / Vulnerability Management 7. Identity Threat Detection & response (ITDR) 8. Decoy/Honeypot/Deception 9. Application security testing tool (DAST/SAST) 10. CSPM Point 1: Experience in 3 solutions – 8 Marks Point 2: Experience in 4 solutions –10 Marks Point 3: Experience in 5 solutions –12 Marks Point 4: Experience in more than 5 solutions– 15 Marks Max Marks – 15 Marks	We request bank to modify the clause and allow 15 marks on 4 and above technologies	Please refer addendum for the revised clause
3591	36		7.3.1.2	EPS measured at SIEM ingestion boundary; XDR-native telemetry not counted if not separately ingested.	For a unified SIEM+XDR platform from the same OEM, kindly clarify how the Bank will verify that XDR-native telemetry is not double-counted. Will OEM certification be accepted as evidence?	Yes. The Bidder shall provide an OEM-certified statement clearly identifying the applicable data flow and licensing/metering methodology. The Bank may use this, along with the required auditable visibility of SIEM-ingested data and native XDR telemetry, to verify that data is not double-counted.
3592	36		7.3.1.2	50,000 EPS / 2.06 TB per day, scalable to 75,000 EPS / 3.09 TB per day.	Kindly confirm whether the licensed capacity is 50,000 EPS or 75,000 EPS, and whether the 75,000 EPS is an optional tranche or included in the base scope.	Please refer addendum for revised clause
3593	37		7.2.4.3	Raw logs 1 month; parsed/normalized logs 60 months on cloud primary storage.	Kindly clarify whether the 60-month retention is on cloud or on the Bank's on-prem long-term storage. If on cloud, please clarify the egress/retrieval cost model.	1. Please refer addendum for the revised clause 2. All required ingress/egress cost is part of the bidder's scope
3594	29		7.2.1	SIEM: Cloud (SaaS) + Hybrid; HA N+N Active-Active at DC and DR.	Kindly clarify whether "N+N Active-Active at DC and DR" means N+N at each site (2+2) or N+N across DC and DR combined (1+1 per site).	Please refer addendum for revised clause
3595	29		7.2.1	Decoy/HoneyPot: Standalone at DC; HA N+N Standalone at DR.	"HA N+N Standalone" is ambiguous. Kindly clarify the HA requirement for the Decoy solution at DC and at DR.	Please refer addendum for revised clause
3596	32		7.2.3	Cloud (SaaS) + Hybrid: CSP-hosted and Bank-hosted components.	Kindly clarify whether the Bank will provide the CSP tenancy (e.g. MeitY-empanelled cloud) or whether the bidder should propose and procure the CSP.	No Change, Please be guided by the RFP. Bidder to propose and procure CSP
3597	38		7.2.4.3	Raw logs retained on Bank-designated primary storage.	Kindly clarify whether the primary storage for on-prem solutions is provided by the Bank or is to be supplied by the bidder.	No Change, Please be guided by the RFP. Bidder to right size and provide all the required infrastrcuture as per RFP
3598	89		7.18	Bidder must size hardware based on Annexure 21 volumetrics.	Kindly share the current infrastructure baseline (existing SIEM EPS, storage utilisation, network throughput) to validate sizing.	Details shall be shared with succesful bidder
3599	92		7.18.3	Backup solution to be sized in accordance with storage sizing.	Kindly share the backup volumetrics (daily change rate, deduplication ratio, retention) to size the backup solution.	Details shall be shared with succesful bidder
3600	123		10.2 (PQ #25)	Minimum 85% per product; S=10, C=3.	Kindly clarify the scoring formula. What is the score for "Not Supported" (is it 0)? How is the percentage computed (sum of S+C over total)?	Score (%) = (Scored Marks / Total Possible Marks) × 100 S (Supported) = 10 marks C (Conditional/Partially Supported) = 3 marks Not Supported = 0 marks Accordingly, the total scored marks will be calculated based on the applicable S/C/Not Supported ratings, and the resulting percentage will be compared against the minimum required score of 85% per product.
3601	95		7.19.2	Bidder to take over existing solutions from 01.05.2027 on an "as-is-where-is" basis.	Kindly share the inventory of existing solutions, OEM contracts, licence status and current SLAs to enable assessment of the transition scope.	details shall be shared with successful bidder
3602	95		7.19.2	Run existing SIEM for 12 months post Go-Live.	Kindly clarify who provides the existing SIEM licences during this 12-month period and whether this is in the bidder's scope.	Yes, the existing SIEM/SOC platform is currently operational and being replaced under this RFP. There will be no data migration from existing SIEM solution. It will runing parallel for for few month to meet the compliance.
3603	149		13.1	RPO 15 min, RTO 60 min; penalty of ₹10,000 per 10 minutes.	Kindly clarify whether RTO/RPO is measured per solution or for the SOC as a whole.	No Change, Please be guided by the RFP Please refer section 13 SERVICE LEVELS & PENALTIES
3604	256		Annexure 21	Current IT assets: 2,500 servers, 300 databases, 200 applications, 12,000 endpoints.	Kindly confirm whether this is the full scope for log ingestion, or whether additional sources (network devices, cloud services) will be added.	The IT asset volumes provided are indicative. The solution shall be sized based on the volumetric requirements specified in the RFP.
3605	69		7.7 (Item 12)	Bank data shall not be used for model training.	Kindly clarify whether anonymised/aggregated data may be used for model improvement, or whether this is a complete prohibition.	No Change, Please be guided by the RFP

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3606	69		7.7 (Item 4)	Support for Bring Your Own Key / Customer-Managed Encryption Key.	Kindly clarify whether the Bank will provide the KMS or whether the bidder should propose one.	Bank is procuring KMS through Separate RFP.
3607	98		9	Overall implementation 5 months from T0.	Kindly clarify whether the 5-month timeline includes UAT and Go-Live, or covers deployment only.	The 5-month timeline covers the complete go-live of the solution, including supply, installation, implementation, and testing.
3608	163		14.14	Local content certificate.	Kindly clarify the minimum local content percentage required for this RFP.	No Changed, Please be guided by the RFP
3609	129		10.3	Technical presentation: 10 marks.	Kindly share the evaluation rubric/criteria for the technical presentation.	Details will be shared once bidder qualifies the eligbility evaluation
3610			10.2 / Annexure 5 (PQ #4)	Minimum average turnover of INR 500 crore per annum in India during the past 3 financial years (2022-23, 2023-24, 2024-25) with positive net worth. Note: in case of MSMEs only, the turnover may be relaxed subject to meeting the quality and technical specifications.	The RFP states turnover "may be relaxed" for MSMEs but does not specify the relaxed threshold. Kindly confirm (a) the specific relaxed turnover value applicable to Udyam-registered MSMEs, (b) whether DPIIT-recognised startups are also covered under this relaxation, in line with GFR 2017 Rule 170 and the Public Procurement Policy for MSEs, and (c) the documents to be submitted (Udyam certificate, DPIIT recognition certificate) to avail the relaxation.	As per 10.2, relaxation applies to MSMEs only, subject to meeting quality and technical specifications
3611			10.2 / Annexure 5 (PQ #6 and #7)	PQ #6: Minimum 100 experienced cybersecurity employees on bidder's payroll. PQ #7: Bidder must have supplied, installed and maintained a SIEM solution of minimum 20,000 EPS / 0.86 TB per day in one PSU/PSE/Government/BFSI/Telecom organisation in India in the last 5 years.	The RFP extends EMD exemption to MSEs and DPIIT-recognised startups but is silent on prior-experience relaxation. Kindly confirm whether Udyam-registered MSMEs and DPIIT-recognised startups are given relaxation on the manpower criterion (PQ #6) and the prior-experience criterion (PQ #7), in line with GFR 2017 Rule 173(i) and DPIIT notifications on relaxing prior-experience and turnover norms for startups. If yes, kindly specify the relaxed thresholds and acceptable proof.	6. Please be guided by the RFP 7. Please refer addendum for revised clause.
3612		APPENDIX 1A Functional Compliance Sheet (Solutions)	NDR Sheet, Point 6	The proposed solution should provide functionality to limit the access to specified IP addresses for accessing the console.	IP Schema keeps on changing in any DC environment, the best practice followed across the industry is to limit the admin/analyst/user access control is through the Role Based access control as mentioned in Point 17 of the specification. **We request PSB bank to please delete the clause as it is not relevant as per the Best Practice followed for access control.**	Please refer addendum for the revised clause
3613		APPENDIX 1A Functional Compliance Sheet (Solutions)	NDR Sheet, Point 13	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability cloud architecture distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead	Natively NDR is not a SAAS or cloud native solution as it ingest the lossless packet within the DC/DR, however console can be hoisted in cloud environment to manage multiple location in high availability, hence we request to change the clause as per NDR fundamental architecture followed accross the industries. "The proposed solution shall feature a centralised console delivering completely customizable security dashboards with dynamic role-based access controls. The underlying dashboard and administration interface must operate in an Active-Active high-availability architecture which can be distributed across multiple availability zones within the designated region, ensuring seamless access from both the Bank's primary and disaster recovery sites with zero local hosting overhead"	Please refer Addendum for revised clause
3614		APPENDIX 1A Functional Compliance Sheet (Solutions)	NDR Sheet, Point 14	Web based GUI and a unified security dashboard displaying the real time consolidated data in graphical/textual format and all alerts received from and detected by all the traffic. The solution should have the ability to view and identify the infected systems and drill down into infection details at centralized location..	EDR/XDR is used to identify and isolate infected endpoints and this feature is not a native feature of NDR hence we requet to delete the following statement from the Specification from the Clause as this make the specs restrictive. "The solution should have the ability to view and identify the infected systems and drill down into infection details at centralized location.. " Please delete this clause above	Please refer addendum for the revised clause
3615		APPENDIX 1A Functional Compliance Sheet (Solutions)	NDR Sheet, Point 18	Solution should have the capabilities to create and run security playbooks for automation and better MTTD/MTTR on the basis of criticality of threat/server	XDR/SOAR has the functionality to create and run playbooks for automation action, NDR can detect and share the alert with SOAR/XDR for action hence this clause is not relevant for NDR, it might be a typo. We request PSB to please delete the clause as this does not applied to NDR solution across the industry and its a restricted clause.	Please refer addendum for revised clause
3616		APPENDIX 1A Functional Compliance Sheet (Solutions)	NDR Sheet,	The specifications provided for NDR does not cover full functionalities and capabilities, the specification only focus on protocol analysis on point 5 which is a partial functionality of NDR solution. For robust cyber security based NDR solution it is imperative to have the following functions for advanced attacks. We request PSB to add following specification for robust NDR solution.	1. NDR should be capable of detecting and protecting from misconfigurations, advanced attacks and malwares that are difficult to detect via signatures like web shell uploads, existing web shells, phishing emails, ransomware, cryptominers, suspicious search prompts for AI portals, network scanning, data exfiltration, lateral movement, malicious attachment, weak password, plain text data containing properity information etc. 2.Capable to provide complete packet-by-packet details of full session of interest including Session reconstruction, Flow analysis, Packet decoding, Web & FTP session reconstruction, artefact & raw packet extractions (for malicious and misconfiguration session). 3.To detect zero day attack the solution must be service agnostic, it must be able to parse and normalize network sessions independent of port or protocol, even for unknown and non-standard protocols. Parsing of known and unknown protocols should be supported with data enrichment (such as threat intelligence feeds and custom business context) must be performed at capture time. 4. The system should provide a feature to extract various types of files from network traffic (.exe,.pdf,.doc,.gif,.jpeg,.wav,.mp3, etc.) and natively anayse the file for any malware.The solution must also be able to extract files from sessions and forwarding them to a 3rd party sandbox. 5. The solution must support to decrypt traffic by importing SSL/TLS private keys, allowing for the decryption of inbound SSL/TLS traffic. The solution must generate fingerprints for	Please refer addendum for the revised clause

S.No.	RFP Page No.	RFP Section Name and No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Pre- bid query Replies
3617		APPENDIX 1A Functional Compliance Sheet (Solutions)	NDR Sheet,	Additional Points	6. Proposed Network Threat Detection platform should adopt technics to provide visibility into malicious channels that are trying to blend in with other traffic (Like RDP using HTTP protocol), but do not follow normal protocol behaviour. Proposed solution should understand the behaviour of the protocol and highlight in case of any discrepancy to undiscovered suspected communication patterns. 7. To create digital evidence the solution must support the full reconstruction of any network session in human readable format. The full network session reconstruction must be supported natively in the console and must not require the download of a PCAP to be opened in a 3rd party application. The soltuion should be able to import PCAP captured by some other solution for analysis. 8.The solution should perform metadata extraction and data enrichment at capture-time this real-time enrichment should include data such as asset information, threat intelligence, business context, indicators of compromise, behaviors of compromise, enablers of compromise, suspicious SSL fingerprints and many other data elements. This data can be used in advanced analytics, investigations, reports … providing context right at the analyst's fingertips. 9.Detect Suspicious traffic from an Unknown or non friendly Country: Meta should provide all details in terms of Country name, location, Business context, IP - From and To Information. Analyst should be able to isolate such traffic swiftly and investigate the payload for any	No Change, Please be guided by the RFP