

पंजाब एण्ड सिंध बैंक

Email: soc.tender@psb.bank.in



Punjab & Sind Bank

Email: soc.tender@psb.bank.in

Addendum 1

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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ

Email: soc.tender@psb.bank.in



Punjab & Sind Bank

Email: soc.tender@psb.bank.in

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.

Addendum 1

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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ Email: soc.tender@psb.bank.in		Punjab & Sind Bank Email: soc.tender@psb.bank.in
--	--	---

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	

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ Email: soc.tender@psb.bank.in		Punjab & Sind Bank Email: soc.tender@psb.bank.in
--	--	---

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	

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ Email: soc.tender@psb.bank.in		Punjab & Sind Bank Email: soc.tender@psb.bank.in
--	--	---

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 Matrix	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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ Email: soc.tender@psb.bank.in		Punjab & Sind Bank Email: soc.tender@psb.bank.in
--	--	---

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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ Email: soc.tender@psb.bank.in		Punjab & Sind Bank Email: soc.tender@psb.bank.in
--	--	---

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)

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ Email: soc.tender@psb.bank.in		Punjab & Sind Bank Email: soc.tender@psb.bank.in
--	--	---

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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ Email: soc.tender@psb.bank.in		Punjab & Sind Bank Email: soc.tender@psb.bank.in
--	--	---

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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ Email: soc.tender@psb.bank.in		Punjab & Sind Bank Email: soc.tender@psb.bank.in
--	--	---

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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ Email: soc.tender@psb.bank.in		Punjab & Sind Bank Email: soc.tender@psb.bank.in
--	--	---

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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ Email: soc.tender@psb.bank.in		Punjab & Sind Bank Email: soc.tender@psb.bank.in
--	--	---

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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ Email: soc.tender@psb.bank.in		Punjab & Sind Bank Email: soc.tender@psb.bank.in
--	--	---

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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ Email: soc.tender@psb.bank.in		Punjab & Sind Bank Email: soc.tender@psb.bank.in
--	--	---

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

Addendum 1

Section 4: Modification in Appendix

Appendix 1A

#	Pre Bid/RFP Reference	Solution Name	Published RFP Specifications	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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ 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 Specifications	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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ 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 Specifications	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 Specifications	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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ 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 Specifications	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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ 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 Specifications	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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ 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 Specifications	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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ 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 Specifications	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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ 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 Specifications	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 IoT 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 mechanism 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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ 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 Specifications	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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ 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 Specifications	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 solution 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 inbuilt 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)

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ 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 Specifications	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 Privilege 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 - Visibility 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 Specifications	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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ 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 Specifications	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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ 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 Specifications	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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ 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 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 offered 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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ 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 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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ 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 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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ 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 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 understand 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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ 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 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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ 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 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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ 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 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, writable 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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ 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 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

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ 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 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