

पंजाब एण्ड सिंध बैंक

Email: soc.tender@psb.bank.in



Punjab & Sind Bank

Email: soc.tender@psb.bank.in

Addendum 2

Updated Addendum 2

DATED [10-10-2026]

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.

Addendum 2

Contents

1. Introduction.....	3
2. Section 1: Modification in RFP Clauses:.....	4
3. Section 2: Updated Section 16.21.2: Volumetrics & Storage Solution-wise Requirements	14
4. Section 3: Updated XDR Specification.....	37
5. Section 4: Updated DRM Specification.....	52
6. Section 5: OEM Undertaking for each proposed solution where authorised partner is engaged by OEM.....	57
7. Section 6: Authorized partner undertaking for each Proposed Solution where authorised partner is engaged.....	60
8. Section 7: Updated ITDR Specification and Eligibility Criteria.....	62
9. Section 8: Updated ITDR Technical OEM Evaluation Criteria.....	66

Addendum 2

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:

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

Addendum 2

2. Section 1: Modification in RFP Clauses:

#	Pre Bid/RFP Reference	Published RFP Clause, Updated RFP Clause (in addendum 1)	Revised RFP Clause/ Clarification
1	Addendum 1, 16.21.2, Volumetrics & Storage Solution-wise Requirements	Volumetrics & Storage Solution-wise Requirements	Refer Section 2 for updated volumetrics
1.	Addendum 1, Appendix 1C, Digital risk management		Refer Section 3 for the updated sheet for DRM specifications (Changes in scoring and re-numbering and deduplication)
2.	Addendum 1, Appendix 1A, XDR		Refer Section 4 for the updated sheet for XDR specifications
3.	Addendum 1, Appendix 1A, XDR, Clauses 51, 53	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. 53. Easy-to-manage, clientless platform that deploys quickly and involves minimal or no dependency on customization and management.	Clarification to the existing clause: The requirement for an easy-to-manage, clientless platform is intended to ensure rapid deployment and minimal dependency on customization and management of the operating environment. The term “clientless” shall not be construed as eliminating or restricting endpoint agents/sensors required for endpoint protection, telemetry collection, investigation and response. Clientless management/analyst access: Admins and analysts access the XDR console through a browser, without installing a desktop client. Administrator and Analyst access shall be through a browser-based interface without dependency on

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

Addendum 2

#	Pre Bid/RFP Reference	Published RFP Clause, Updated RFP Clause (in addendum 1)	Revised RFP Clause/ Clarification
			thick clients, plug-ins or local installation, wherever specified in the RFP.
4.	Addendum 1, Appendix 1A, XDR, Clause 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.	Clarification to the existing clause: The proposed solution shall provide host-level firewall capability with stateful inspection and the specified policy criteria including Source, Destination, Port, Protocol and Application. The specified network virus/malware scanning capability shall also be provided through the appropriate component of the proposed architecture. The requirement does not mandate that network virus/malware scanning be performed exclusively by the endpoint agent.
5.	Addendum 1, Appendix 1A, XDR, Clause 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.	Clarification to the existing clause: The Bank has deliberately specified high-speed lossless packet capture and analysis for 10 Gbps to meet its required Detection, Network Visibility, Investigation, Forensic and Back-in-Time Investigation capabilities. The Bidder shall propose a solution capable of meeting the requirement as published. The requirements specified under NDR Points 1 to 15 of Addendum 2 pertain to NDR (Network Detection and Response) capabilities. The Bidder may meet these requirements either through NDR functionality integrated within the proposed XDR solution (single OEM) or through a separate NDR solution integrated with the proposed XDR solution (separate XDR and NDR OEMs), provided that the proposed architecture

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

Addendum 2

#	Pre Bid/RFP Reference	Published RFP Clause, Updated RFP Clause (in addendum 1)	Revised RFP Clause/ Clarification
			delivers the complete functionality and outcomes specified under NDR Points 1 to 15. In all cases, the NDR and XDR capabilities shall be delivered as an integrated solution. PQ/TQ applicability shall be as follows: - Where XDR and NDR are proposed from separate OEMs: The XDR OEM and NDR OEM shall both independently meet the applicable PQ requirements specified in the RFP. However, the applicable TQ Scoring requirements shall be evaluated only for the XDR OEM. - Where XDR & NDR is proposed from a single OEM: The single XDR OEM shall meet the applicable XDR PQ and TQ requirements specified in the RFP. Where a separate NDR solution is proposed, the Commercial BOM shall clearly identify XDR and NDR as separate line items, specifying the respective OEM, solution/component details, quantities and associated costs.
6.	Addendum1, Appendix 1A, CNAPP, Clause 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.	The solution shall provide capabilities to map applications and workloads to their underlying cloud services, resources, identities, dependencies and application components, enabling application-level security analysis.
7.	Addendum1,	The solution shall provide visibility into application dependencies and software components and shall	The solution shall provide visibility into application dependencies and software components and shall identify

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

Addendum 2

#	Pre Bid/RFP Reference	Published RFP Clause, Updated RFP Clause (in addendum 1)	Revised RFP Clause/ Clarification
	Appendix 1A, CNAPP, Clause 18	identify affected applications where a vulnerable component or dependency is detected.	affected applications and workloads where a vulnerable component or dependency is detected.
8.	Addendum1, Appendix 1A, CSPM, Clause 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	The solution must provide 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
9.	Addendum1, Appendix 1A, CTEM, Clause 7	Each intelligence item should include metadata such as date, author, source etc.	Each intelligence item should include metadata such as date, source, threat context, and classification of the available intelligence data.
10.	Addendum1, Appendix 1A, CTEM, Clause 39	The solution should integrate via APIs with the existing security stack including NGFW, WAF, XDR, and UEM platforms and other relevant security controls.	The solution should integrate via APIs or supported integration mechanisms with the existing security stack, including NGFW, WAF, XDR, UEM platforms and other relevant security controls.
11.	Addendum1, Appendix 1A, CTEM, Clause 55	The solution should include IOC investigation, infrastructure mapping, and threat actor identification	The solution should include threat intelligence investigation, infrastructure mapping, and threat actor identification.
12.	Addendum1, Appendix 1A, VA-VM, Clause 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.	Clause stands deleted

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

Addendum 2

#	Pre Bid/RFP Reference	Published RFP Clause, Updated RFP Clause (in addendum 1)	Revised RFP Clause/ Clarification
13.	Addendum1, Appendix 1B, Primary Storage, Clause 3	The proposed array should be an unified storage which support both SAN & NAS	The proposed storage array shall support SAN (Mandatory) and/or NAS.
14.	Addendum1, Appendix 1B, Primary Storage, Clause 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, NVMe/TCP, NVMe/FC from day one. If the bidder architecture requires NAS also, then the proposed array should also support (NFS v4.0 or above) / (SMB 3.1 or above).
15.	Addendum1, Appendix 1B, Backup Solution, Clause 16	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	The proposed disk-based storage/appliance must interoperate with industry leading server platforms and operating systems, and must ingest backup data over a secure, using standard data protocols such as FC, iSCSI, NFS, S3 or API-based disk-to- disk (D2D) connection.
16.	Addendum1, Appendix 1B, Backup Solution, Clause 18	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	The proposed Disk Based Appliance/Backup Storage should have the capability to tier backup data to external storage (on-premise). The capability for tiering backup data to external storage may be provided through the overall proposed Backup Solution, including the backup software and/or storage/appliance components, as applicable to the proposed architecture, provided that the tiered backup data remains appropriately managed, identifiable and recoverable. All licenses required for such functionality shall be provided from 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

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

Addendum 2

#	Pre Bid/RFP Reference	Published RFP Clause, Updated RFP Clause (in addendum 1)	Revised RFP Clause/ Clarification
		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	should have minimum of 4 × 16/32G FC ports and "either 2 × 32G FC ports or 4 × 10/25GbE network ports" on each controller on each controller for Host connectivity. Proposed Backup Solution should have minimum 4x scalability of the current quoted capacity for future growth.
17.	Addendum1, Appendix 1B, Backup Solution, Clause 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 Bank's existing requirement is intentionally worded to ensure that the bidder factors all applicable overheads—including memory, capacity, technology and IOPS. Give me enough backup capacity and processing power so that, even after deduplication and with multiple backup pools running, all my scheduled backups can finish within 8 hours without the system becoming slow.
18.	Addendum1, Appendix 1B,	Proposed Appliance/Backup Storage should support different retentions for primary and DR backup storage and should support instant copy creation on	Clarification to the existing clause: The sought capabilities may be provided through the overall proposed Backup Solution, including backup software and/or

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

Addendum 2

#	Pre Bid/RFP Reference	Published RFP Clause, Updated RFP Clause (in addendum 1)	Revised RFP Clause/ Clarification
	Backup Solution, Clause 21	remote site for better DR readiness with support for transmitting only deduplicated unique data in encrypted format to remote sites.	backup appliance/storage components, as applicable to the proposed architecture, while meeting the stated requirements Where any of the above capabilities are provided through the backup software, appliance, storage or a combination thereof, the bidder shall provide the complete end-to-end functionality without requiring additional components or licenses beyond those quoted in the proposed solution.
19.	-	Additional	Bidder may utilise the OEM Authorized partner for the following: The implementation of the proposed solution may be undertaken by the OEM/OEM Authorised Partner, covering design, installation, configuration, integration, migration, testing, commissioning, UAT and Go-Live. However, all applicable terms, conditions, obligations and requirements of the RFP, including the confidentiality, security, compliance and other obligations specified in the prescribed Undertakings, shall remain fully applicable and shall be duly fulfilled and complied with by the Bidder, OEM and Authorised Partner. All other terms and conditions of the RFP shall remain unchanged Where the bidder proposes to adopt the OEM Authorised Partner-led implementation approach, the bidder shall submit the prescribed OEM Undertaking (<u>Section 5: OEM Undertaking for each proposed solution where partner is engaged by OEM</u>) and Authorised Partner Undertaking (<u>Section 6: Authorised Partner undertaking for each proposed</u>

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

Addendum 2

#	Pre Bid/RFP Reference	Published RFP Clause, Updated RFP Clause (in addendum 1)	Revised RFP Clause/ Clarification
			<u>solution where authorised partner is engaged by OEM)</u> along with its bid. Failure to submit the required undertaking(s) shall render the bid liable for rejection as non-responsive.
20.	OEM Evaluation Criteria Point 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 maintaining that solution or has carried out its maintenance at any time during the five-year period preceding the RFP publication date	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. Application Security testing Tool (SAST & DAST) 4. Cloud Security solution (CSPM) The proposed OEM solution should have been implemented in at least one Scheduled Commercial Bank/PSU/ PSE/Government Organizations / BFSI/ At least one verifiable client in India. . Credential is to be submitted for the following solution: 1 Identity threat detection and response (ITDR) 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 maintaining that solution or has carried out its maintenance at any time during the five-year period preceding the RFP publication date

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

Addendum 2

#	Pre Bid/RFP Reference	Published RFP Clause, Updated RFP Clause (in addendum 1)	Revised RFP Clause/ Clarification
21.	Addendum 1 Appendix 1A ITDR clause 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	Clause Stands Deleted
22.	Addendum 1 Clause 10.3 Technical Evaluation Criteria S.No.4 OEM Evaluation Criteria	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: 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	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. Application Security testing Tool (Both DAST & SAST) 8. Cloud Security posture Management tool(CSPM) And The proposed OEM solution (solution list in mentioned below) should have been implemented in Client (BFSI/PSU/PSE/ Govt Organization/ At least one verifiable client) in India. Bidder to substantiate the clause for each of the below-mentioned solution and scoring for each of the solution

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

Addendum 2

#	Pre Bid/RFP Reference	Published RFP Clause, Updated RFP Clause (in addendum 1)	Revised RFP Clause/ Clarification
		out its maintenance at any time during the five-year period preceding the RFP publication date	would be summed to arrive at the solution OEM experience score. List of Solutions are: 1. Identity Theft Detection & response 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

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

Addendum 2

3. Section 2: Updated Section 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 / “2.73 TB/day”, whichever is higher, at DC & DR.	Scalable up to 100,000 sustainable EPS / “5.44 TB/day”, whichever is higher. Additional capacity in tranches of 10,000 EPS / “544 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. An average raw event size of 630 bytes (uncompressed) The bidder shall provide the Bank with a on-premises tool to showcase the flow of data from Bank sites to the cloud-hosted SIEM. The tool shall provide visibility of the actual data volume transmitted and shall enable calculation of the corresponding EPS/ data ingestion volume.
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.

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

Addendum 2

Solution Name	Day-1 Requirement	Scalability / Pro-Rata Requirement	Other Mandatory Requirements
User & Entity Behaviour Analytics (UEBA)	Minimum 50,000 sustainable EPS / “2.73 TB/day”, whichever is higher, at DC & DR; 12,000 endpoint users.	Scalable up to 100,000 sustainable EPS / “5.44 TB/day”, whichever is higher and 16,000 endpoint users. Additional capacity in tranches of 500 endpoints at quoted BOM rates.	
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	Scalable up to 16,000 users/endpoints.	

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

Addendum 2

Solution Name	Day-1 Requirement	Scalability / Pro-Rata Requirement	Other Mandatory Requirements
	comprehensive visibility across key network aggregation points	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.	
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.	

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

Addendum 2

Solution Name	Day-1 Requirement	Scalability / Pro-Rata Requirement	Other Mandatory Requirements
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.	
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.

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

Addendum 2

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.	The Bidder may provide primary raw-log storage either on-premises or on cloud, based on the proposed solution architecture. However, the solution shall mandatorily retain a minimum of 3 months of raw logs .	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.
	Processed Log Storage on Cloud	Parsed, normalized, enriched, indexed and correlated logs, including associated metadata and context, shall be retained.	Hot Storage – 6 Months: The most recent 6 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 – 24 Months: The subsequent 24 months of processed logs shall be maintained in Warm Storage and shall remain searchable and retrievable with minimum latency to support historical investigation, threat	1. Logs shall remain searchable and retrievable. 2. Adequate storage shall be provisioned for indexing, enrichment and growth. 3. Historical investigation shall be supported.

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

Addendum 2

Solutions	Components	Requirements	Period	Details
			hunting, compliance and forensic requirements.	
	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. Bank-owned SIEM data shall be backed up to Bank-designated DC & DR Backup. This shall include 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	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. 6. No additional license, software, transfer, retrieval or restoration charges shall apply

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

Addendum 2

Solutions	Components	Requirements	Period	Details
		archived on the Bank's infrastructure (i.e., Long-Term Storage)		
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	1. Data shall remain searchable and retrievable. 2. Historical investigation shall be supported. 3. 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. On-premise: 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,	As backup & retention Policy	

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

Addendum 2

Solutions	Components	Requirements	Period	Details
		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	1. Searchable and retrievable. 2. Historical investigation and behavioural analysis shall be supported. 3. Adequate storage for growth shall be provisioned.
	Backup	On-Cloud: UEBA application-specific configurations, policies, detection models/rules, dashboards, workflows and 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	As backup & retention Policy	1. Secure backup. 2. Required backup/data-transfer utilities included. 3. Restoration as per RTO/RPO. 4. Quarterly testing. 5. No additional charges.

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

Addendum 2

Solutions	Components	Requirements	Period	Details
		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 information shall be retained on Cloud/CSP infrastructure.	Minimum 3 Months	1. Searchable and retrievable. 2. Historical investigation shall be supported. 3. Storage shall account for ingestion and growth.
	Backup	On-Cloud: XDR policies, detection rules, configurations, dashboards,	As backup & retention Policy	1. Secure backup.

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

Addendum 2

Solutions	Components	Requirements	Period	Details
		workflows and user/role configurations shall be backed up on Cloud/CSP. On-premises: 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)		2. Required connectors/APIs/utilities included. 3. Restoration as per RTO/RPO. 4. Quarterly restoration testing. 5. No additional charges.

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

Addendum 2

Solutions	Components	Requirements	Period	Details
TIP	Primary Data Storage on cloud	Threat Intelligence data, IoCs, threat actors, campaigns, relationships, enrichment, sightings, investigations, metadata and associated intelligence shall be retained on Cloud/CSP infrastructure.	Minimum 3 Months	- Intelligence shall remain searchable and retrievable. - Historical intelligence shall be available for 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	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.

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

Addendum 2

Solutions	Components	Requirements	Period	Details
		trails available to the Bank. The audit trails shall be backed up and archived on the Bank's infrastructure (i.e., Long-Term Storage)		
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	As backup & retention Policy	• Secure backup. • Restoration as per RTO/RPO. • Required utilities included. • Quarterly testing. • No additional charges.

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

Addendum 2

Solutions	Components	Requirements	Period	Details
		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)		
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	As backup & retention Policy	• Secure backup. • Required APIs/connectors included. • Restoration as per RTO/RPO. • Quarterly testing. • No additional charges.

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

Addendum 2

Solutions	Components	Requirements	Period	Details
		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)		
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	As backup & retention Policy	• Secure backup. • Restoration as per RTO/RPO. • Required utilities included.

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

Addendum 2

Solutions	Components	Requirements	Period	Details
		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 shall be backed up and archived on the Bank's infrastructure (i.e., Long-Term Storage)		• Quarterly testing. • No additional charges.
CTEM	Primary Data Storage on cloud	Exposure findings, vulnerabilities, attack-path information, asset information, risk/prioritization data, validation results, remediation status and associated metadata	Minimum 3 Months	• Historical exposure information shall be searchable and retrievable. • Historical assessment and remediation tracking shall be supported.

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

Addendum 2

Solutions	Components	Requirements	Period	Details
		shall be retained on Cloud/CSP infrastructure.		
	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 to the Bank. The audit trails shall be backed up and archived on the Bank's	As backup & retention Policy	• Secure backup. • Required APIs/connectors/utilities included. • Restoration as per RTO/RPO. • Quarterly testing. • No additional charges.

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

Addendum 2

Solutions	Components	Requirements	Period	Details
		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,	As backup & retention Policy	- Secure backup. - Restoration as per RTO/RPO. - No additional charges.

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

Addendum 2

Solutions	Components	Requirements	Period	Details
		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) 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		

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

Addendum 2

Solutions	Components	Requirements	Period	Details
		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 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.	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
	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,	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.

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

Addendum 2

Solutions	Components	Requirements	Period	Details
		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 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,		No additional license/software/backup/restoration charges.

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

Addendum 2

Solutions	Components	Requirements	Period	Details
		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)		
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,	Minimum 3 Months	• Data shall remain searchable and retrievable. • Historical identity-threat investigation shall be supported. • Adequate storage shall be provisioned for data growth.

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

Addendum 2

Solutions	Components	Requirements	Period	Details
		detection results, investigation data, 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, 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, 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	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.

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

Addendum 2

Solutions	Components	Requirements	Period	Details
		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 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**

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

Addendum 2

4. Section 3: Updated XDR Specification

S.No	Updated Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
A. Extended Detection and Response (XDR)					
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	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.	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.	10	Select	0	
4	It should have but following prevention capabilities:	-	-	-	
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 remodelled 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	

Addendum 2

S.No	Updated Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
4.2	• Ransomware protection	10	Select	0	
4.3	• Machine learning - pre-execution and runtime / Signature-less	10	Select	0	
4.4	• Browser exploit protection	10	Select	0	
4.5	• Behavior monitoring	10	Select	0	
4.6	• Polymorphic attack prevention	10	Select	0	
4.7	• Script protection	10	Select	0	
4.8	• Anti-exploit	10	Select	0	
4.9	• C&C communication prevention	10	Select	0	
4.10	• File less malware prevention	10	Select	0	
4.11	• File reputation	10	Select	0	
4.12	• Sandboxing of files	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	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	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.	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.	10	Select	0	

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

Addendum 2

S.No	Updated Functionalities/Features	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	10	Select	0	
9	The proposed solution is a fully managed, cloud-native SaaS platform that guarantees 99.9% uptime"	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	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.	10	Select	0	
12	The proposed solution must provide protection against malicious AI application tampering on the endpoints	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	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.	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.	10	Select	0	

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

Addendum 2

S.No	Updated Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
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.	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	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	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).	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.	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.	10	Select	0	

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

Addendum 2

S.No	Updated Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
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	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.	10	Select	0	
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.	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.	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.	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.	10	Select	0	
28	The solution shall support host-based firewall capabilities for controlling network traffic and provide network-based malware detection and prevention through native or integrated endpoint security components.	10	Select	0	

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

Addendum 2

S.No	Updated Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
29	The solution Device Control capability must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, and Deny Access. The solution Device Control capability must support, USB, Mobile Storage, Bluetooth adapter, printer, capabilities allowing admin to define the policy specifically for the endpoint operating systems (Windows 10, 11 or higher).	10	Select	0	
30	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).	10	Select	0	
31	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.	10	Select	0	
32	Should allow the creation of custom detection models and custom event filters that define the events the model uses to trigger alerts.	10	Select	0	
33	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 analyzing the logs of endpoint protection solution	10	Select	0	
34	The console should provide different search methods, filters, and an easy-to-use Kibana-like query language or	10	Select	0	

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

Addendum 2

S.No	Updated Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
	any other query language to identify, categorize, and retrieve search results and				
35	The proposed solution 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.	10	Select	0	
36	The proposed solution must provide the below response capabilities	-	-	-	
36.1	Remotely connect to an endpoint and dump process memory.	10	Select	0	
36.2	Remote isolation of an endpoint but still maintain communication with the management server to continue with investigation.	10	Select	0	
36.3	Ability to remotely connect and execute custom PowerShell or Bash scripts.	10	Select	0	
36.4	Remote shell session capability and be able to execute remote commands	10	Select	0	
36.5	Submit selected file or object for automated analysis in a sandbox, a secure virtual environment.	10	Select	0	
36.6	Ability to view and terminate active processes on a specific endpoint or multiple endpoints.	10	Select	0	
37	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.	10	Select	0	
38	To optimize the bandwidth solution should support update agent/edge relay/peer relay where one or more endpoints can download component updates and push it to other endpoints in PSB environment	10	Select	0	

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

Addendum 2

S.No	Updated Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
39	Solution should offer customizable level of degree of vigilance and strictness applied when detecting and responding to potential threats via the detection & response sensor	10	Select	0	
40	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.	10	Select	0	
41	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.	10	Select	0	
42	The proposed solution must include functionality to perform sandbox analysis of suspicious files, provided as a native capability	10	Select	0	
43	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.	10	Select	0	
44	The proposed solution must allow administrators to manage and control temporary exceptions for trusted devices if needed	10	Select	0	
45	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	10	Select	0	

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

Addendum 2

S.No	Updated Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
46	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.	10	Select	0	
47	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.	10	Select	0	
48	The proposed XDR solution should provide AI-assisted investigation capabilities to support analysts with threat analysis, contextual insights, investigation guidance, and response recommendations.	10	Select	0	
49	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.	10	Select	0	
50	Bidders must propose a solution which is easy-to-manage, clientless platform that gets deployed quickly and involves minimal or no dependency on	10	Select	0	

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

Addendum 2

S.No	Updated Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
	customization and management of operating environment.				
51	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.	10	Select	0	
52	Easy-to-manage, clientless platform that deploys quickly and involves minimal or no dependency on customization and management.	10	Select	0	
53	Perimeter Analytics should have well defined work flow for response mechanism along with integration from F/w, XDR, SOAR and SIEM	10	Select	0	
54	The solution should provide a API and should be integrated with security orchestration (SOAR) to implement response actions.	10	Select	0	
55	Support SNMP/syslog etc. for integration with all leading SIEM/SOC solutions. The Solution components should also be providing access over 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.	10	Select	0	
56	The proposed solution shall feature a cloud-native SaaS console delivering completely customizable security dashboards with dynamic role-based access controls.	10	Select	0	

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

Addendum 2

S.No	Updated Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
	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				
57	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.	10	Select	0	
58	Central management solution must have capability to enable remote management and configurations	10	Select	0	
60	Solution should be able to integrate with 3rd party solution like:	-	-	-	
60.1	ITSM	10	Select	0	
60.2	SIEM	10	Select	0	
60.3	UEM and UEBA	10	Select	0	
60.4	Vulnerability Management/UEBA	10	Select	0	
60.5	Any other security solution	10	Select	0	
61	Proposed Solution should offer granular role-based access control policy for accessing the console	10	Select	0	
62	Solution should have the capabilities to create and run security playbooks for automation and better MTTR/MTTD on the basis of criticality of threat/server	10	Select	0	
63	Solution should provide out of the box report both on the console as well as over email in CSV, PDF or RTF format	10	Select	0	
64	The proposed solution should have centralized management	10	Select	0	

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

Addendum 2

S.No	Updated Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
65	The solution will offer a 360-degree identity view for all users and systems, providing a comprehensive understanding of their attributes, access, and historical behaviour.	10	Select	0	
NDR					
1	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	
2	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	
3	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	
4	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	10	Select	0	

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

Addendum 2

S.No	Updated Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
	isolation, firewall/security-control policy updates and initiation of automated response workflows, wherever supported by the proposed architecture.				
5	The proposed solution shall support integration with the Bank's SIEM and SOAR platforms through standard interfaces, including APIs, Syslog and other industry-standard mechanisms, for exchange of network alerts, incidents, Indicators of Compromise, telemetry and response actions.	10	Select	0	
6	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	
7	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	
8	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	
9	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	

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

Addendum 2

S.No	Updated Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
10	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	
11	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	
12	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	
13	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	
14	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	
15	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.	10	Select	0	

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

Addendum 2

S.No	Updated Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
	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.				
TOTAL MARKS		1040		0	

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

Addendum 2

5. Section 4: Updated Digital risk management (DRM) Specification

Digital risk management					
S.No.	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
Anti-Phishing					
1	Anti-phishing and domain monitoring services	10	Select	0	
2	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	
3	The Bidder should not face obstruction in their activity regardless of international border & language	10	Select	0	
4	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	
5	Bring down the reactivated phishing site at earliest which was earlier detected as phishing site	10	Select	0	
6	The Bidder should track new domain name registrations to detect any spoofed site being Registered	10	Select	0	
7	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	
8	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	
9	The Bidder should monitor any fraudulent mobile applications targeting Bank Bank's customers to capture their credentials for fraudulent transactions	10	Select	0	
10	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	
11	The Bidder should monitor and log all phishing attempts	10	Select	0	

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

Addendum 2

Digital risk management					
S.No.	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
12	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	
13	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	
14	The Bidder should monitor similar domain name registrations	10	Select	0	
15	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	
16	Anti-phishing and domain monitoring services	10	Select	0	
17	Compliance with regulatory advisory on phishing attacks	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	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	
22	The Bidder/OEM should be member of Anti-Phishing Working Group (APWG) or an equivalent international cybersecurity industry affiliation.	10	Select	0	
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.	10	Select	0	
24	The Bidder should monitor any fraudulent mobile applications targeting Bank Bank's customers to capture their credentials for fraudulent transactions	10	Select	0	
25	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	
26	The Bidder should monitor and log all pharming and phishing attempts	10	Select	0	
27	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	

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

Addendum 2

Digital risk management					
S.No.	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
28	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	
29	The Bidder should monitor similar domain name registrations	10	Select	0	
30	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	
31	Bring down the reactivated phishing site at earliest which was earlier detected as phishing site	10	Select	0	
32	The Bidder should track new domain name registrations to detect any spoofed site being Registered	10	Select	0	
33	The Bidder should not face obstruction in their activity regardless of international border & language	10	Select	0	
34	Bidder should be able to take counter measures including (but not limited to)				
34.1	Bring websites down that are capable of causing phishing attacks	10	Select	0	
34.2	Baiting	10	Select	0	
34.3	Notify various internet browsers about detected sites for blocking these at browser level.	10	Select	0	
34.4	Bidder must have capability for monitoring of look-alike domain name registrations and alerting the Bank in case of detection	10	Select	0	
34.5	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	
Brand Abuse					
35	Social media threat protection services	10	Select	0	
36	Identification of account impersonation activity	10	Select	0	
37	Monitoring all major mobile app marketplaces for counterfeit, copycat apps, or apps infringing trademarks	10	Select	0	
38	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	
39	Monitor for Brand mentions in sources Messaging platforms like Telegram, Discord, Facebook, Twitter, Instagram etc. (if any)	10	Select	0	

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

Addendum 2

Digital risk management					
S.No.	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
40	Monitoring potential logo abuse for organization logo (if any)	10	Select	0	
41	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	
42	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	
43	The platform should offer Top Executives/VIP account monitoring	10	Select	0	
44	The platform should be able to identify account impersonation	10	Select	0	
45	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	
46	Identify any fake apps / sites / scam / misinformation in the name of Company.	10	Select	0	
47	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	
48	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	
49	Brand abuse services	10	Select	0	
50	Social media threat protection services	10	Select	0	
51	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	
52	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.	10	Select	0	

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

Addendum 2

Digital risk management					
S.No.	Updated in Addendum	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
	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				
53	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	
54	Identification of account impersonation activity	10	Select	0	
55	The Bidder should provide for identification of fake recruitment schemes claiming affiliation with the Bank	10	Select	0	
55.1	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	
55.2	Prompt submission of enforcement notices and for the removal of rogue or infringing applications	10	Select	0	
55.3	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	
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	

Addendum 2

6. Section 5: OEM Undertaking for each proposed solution where authorised partner is engaged by OEM

(To be issued on the official letterhead of the Solution OEM)

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,

Subject: OEM Undertaking for Authorised Partner-led Implementation and End-to-End OEM Responsibility in reference to the Request for proposal for Selection of bidder for supply installation, implementation, maintenance & management of NextGen SOC & related services

Dear Sir/Madam,

With reference to the RFP "[RFP Name]", RFP No. [____], we, [OEM Legal Name], having our registered office at [____], hereby confirm and undertake as follows:

1. Authorised Partner

We confirm that [Partner Name], other than the bidding partner, is our duly authorised [Highest Partner Status] Partner for [Solution/Product] and is authorised to undertake implementation and professional services for the proposed solution under the above RFP

2. Implementation Experience

We confirm that the above authorised partner has successfully implemented proposed solution name <____> on [Cloud Platform, if cloud is proposed or on-premises, if on-premises is proposed in bank's RFP] for at least one client in India.

- Client Name: _____
- Location: _____
- Scope of Implementation: _____
- Year of Go-live: _____
- Current Status: _____

We confirm that the above information is accurate and may be independently verified by the Bank with the stated client.

3. Client Feedback / Reference

We confirm that the above implementation was undertaken by the above-mentioned partner and authorise the Bank to obtain feedback from the stated client regarding the Partner's implementation capability and performance.

4. OEM End-to-End Responsibility

Addendum 2

<OEM Name: _____> shall retain full and end-to-end responsibility and accountability for the proposed solution throughout the contract period, irrespective of the Partner's involvement. The Partner's engagement shall not limit, transfer or dilute any OEM obligation under the RFP or resulting contract.

Engagement of the authorised Partner shall not limit, transfer, dilute or otherwise affect any responsibility or obligation of the OEM under the RFP or the resulting contract.

5. Scope of Partner's Role

The authorised Partner may undertake the implementation and professional services activities permitted under the RFP, up to and including Go-Live. Such activities shall be performed strictly in accordance with the OEM's prescribed implementation methodology, technical standards, security requirements and instructions, and the Bank's approved requirements.

All deliverables prepared by the partner shall be reviewed, technically validated and signed/ approved by authorised OEM personnel before submission to the Bank. For each final deliverable, the OEM shall provide written confirmation that the deliverable has been reviewed and validated, conforms to the OEM's applicable standards and approved architecture, and is fully accepted and owned by the OEM.

The Partner's involvement in implementation shall therefore not dilute or transfer the OEM's responsibility for any deliverable, implementation activity or the overall performance of the proposed solution.

6. Post-Go-Live OEM Responsibility

We specifically confirm that all obligations relating to annual review, product support, warranty, ATS/AMC, upgrades, patches, vulnerability remediation, security, compliance, product lifecycle, technical escalation, performance, defect resolution and other OEM obligations shall remain the direct responsibility of <OEM Name_____> throughout the contract period.

7. OEM Technical Support and Escalation

We shall provide direct OEM-level technical support and escalation, including for critical technical, security, integration, performance, product and compliance matters.

8. Compliance and Performance:

We undertake that the proposed solution shall comply with the applicable requirements of the RFP and that the Partner's involvement shall not affect the OEM's obligation to ensure successful delivery and performance of the solution.

No back-to-back, teaming, or other arrangement between the OEM, Bidder and/or OEM authorised Partner shall create any additional obligation, liability or payment responsibility on the Bank beyond the terms of the RFP and the resulting contract.

9. Verification

We authorize the Bank to verify this undertaking, our Partner's authorization status and the stated client implementation reference directly with [OEM Name], [Partner Name] and/or the stated client.

10. Binding Undertaking:

Addendum 2

This undertaking is issued specifically for the above RFP and shall be binding upon <_____ OEM Name>. The OEM shall remain responsible for all obligations attributable to the Solution OEM under the RFP and resulting contract, notwithstanding the appointment or involvement of an authorised Partner.

For and on behalf of

OEM Name _____

Authorised Signatory

Name: _____

Designation: _____

Signature: _____

Company Seal: _____

OEM Authorisation/Partner ID: _____

Email: _____

Telephone: _____

The OEM shall provide a **publicly accessible link to the OEM's official partner directory/partner locator or other official online source** through which the Bank can independently verify the Partner's current authorisation and partner status. The link shall specifically identify the Partner and the applicable partner tier/status, wherever such information is publicly available.

Solutions Eligible for Authorised Partner / OEM Professional Implementation:

The following solutions may be implemented by either the **respective Solution OEM or its duly authorised Partner**, subject to all conditions specified in the RFP and the OEM undertaking:

1. SIEM
2. SOAR
3. UEBA
4. Extended Detection & response (XDR)
5. Network Detection & response (NDR)
6. Decoy/HoneyPot/Deception
7. Threat Intelligence Platform
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)

The above flexibility shall be limited to **implementation and professional services up to and including Go-Live**.

Addendum 2

7. Section 6: Authorized partner undertaking for each Proposed Solution where authorised partner is engaged

To be issued on the official letterhead of the Solution Authorised Partner 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

Dear Sir,

Subject: Authorised Partner Undertaking for Authorised Partner-led Implementation and End-to-End OEM Responsibility in reference to the Request for proposal for Selection of bidder for supply installation, implementation, maintenance & management of NextGen SOC & related services

We, [Authorised Partner name _____], confirm that we are an authorised [Highest Partner Level] Partner of _____ for [Solution Name] and have successfully implemented the said OEM's solution in India for _____ on _____. The below implementation may be independently verified by the Bank.

- a. Client Name: _____
- b. Location: _____
- c. Scope of Implementation: _____
- d. Year of Go-live: _____
- e. Current Status: _____

We confirm that the above information is accurate and may be independently verified by the Bank with the stated client.

Where engaged under the RFP, we undertake to perform the permitted implementation services activities up to and including Go-Live in accordance with the OEM's prescribed methodology, technical standards and instructions and the Bank's approved requirements.

We shall be directly and equally accountable for the quality, correctness, security, compliance and timely performance of all activities and deliverables undertaken by us, and shall comply with all applicable RFP requirements, NDA, security/confidentiality, terms, obligations and provide all required documents, evidence and deliverables.

We shall remain responsible for any act, omission, breach or non-compliance attributable to us or our personnel in connection with the services performed under the RFP as per the terms of the RFP.

ਪੰਜਾਬ ਐਂਡ ਸਿੰਧ ਬੈਂਕ

Email: soc.tender@psb.bank.in



Punjab & Sind Bank

Email: soc.tender@psb.bank.in

Addendum 2

We shall be directly accountable for all activities and deliverables undertaken by us and shall comply with all applicable provisions of the RFP, including security, confidentiality, data protection, audit, documentation and compliance requirements. We shall execute the required NDA/confidentiality undertaking directly with the Bank and shall ensure that our personnel comply with the same.

For and on behalf of

Authorised Partner Name _____

Authorised Signatory

Name: _____

Designation: _____

Signature: _____

Company Seal: _____

OEM Authorisation/Partner ID: _____

Email: _____

Telephone: _____

Addendum 2

8. Section 7: Updated ITDR Specification and Eligibility Criteria

Existing Clause of Eligibility Criteria of ITDR

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 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. • 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 clientissued document, the Bidder may submit a combination of client issued documents, provided that together they establish compliance with the eligibility criteria.
------------	--	---

Addendum 2

		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: 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.
--	--	--

Modified Clause of Eligibility Criteria of ITDR

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. Application Security testing Tool (SAST & DAST) 4. Cloud Security solution (CSPM) The proposed OEM solution should have been implemented in at least one Scheduled Commercial Bank/PSU/ PSE/Government Organizations / BFSI/ At least one verifiable client in India. . Credential is to be submitted for the following solution: 1 Identity threat detection and response (ITDR)	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;
-----	--	---

Addendum 2

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 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. 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 clientissued 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:
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.

Addendum 2

		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.

Updated Eligibility Criteria of ITDR

Addendum 1 Appendix 1A ITDR clause 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 the	Clause Stands Deleted
--	--	-----------------------

*Other points as per addendum 1 remains same.

Addendum 2

9. Section 8: Updated ITDR Technical OEM Evaluation Criteria

Existing Clause of Technical OEM Evaluation Criteria of ITDR

S.No	Criteria	Scoring
OEM Evaluation Criteria		
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: 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 = 2 Marks Point 2 = 3 Marks Max Marks – 27 Marks

Modified Clause of Technical OEM Evaluation Criteria of ITDR

S.No	Criteria	Scoring
OEM Evaluation Criteria		
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. Application Security testing Tool (Both DAST & SAST) 8. Cloud Security posture Management tool(CSPM) And	Point 1 = 2 Marks Point 2 = 3 Marks Max Marks – 27 Marks

Addendum 2

	The proposed OEM solution (solution list in mentioned below) should have been implemented in Client (BFSI/PSU/PSE/ Govt Organization/ At least one verifiable client) 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. Identity Theft Detection & response 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	
--	---	--