Addendum - 01

Published on: 25th March 2026

ੴ ਸ੍ਰੀ ਵਾਹਿਗੁਰੂ ਜੀ ਕੀ ਫ਼ਤਹਿ

Punjab & Sind Bank

(A Govt. of India Undertaking)

Where service is a way of life

REQUEST FOR PROPOSAL

FOR

SELECTION OF CERT-IN EMPANELED BIDDER FOR PROVIDING CYBER SECURITY SERVICES (CSS)

BID NO: PSB/ HO-CISO CELL/2026/SERVICES RFP DATED 20/02/2025

GEM/2026/B/7271228

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

Punjab & Sind Bank
(A Govt. of India Undertaking)
Where service is a way of life

Addendum – 01

Introduction

Bank has published the RFP vide BID NO: PSB/ HO-CISO CELL/2026/SERVICES RFP DATED 20/02/2025 for SELECTION OF CERT-IN EMPANELED BIDDER FOR PROVIDING CYBER SECURITY SERVICES (CSS). 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.

In reference to the aforesaid RFP, all are advised to note following

S. No	Page No.	RFP Section No.	RFP Existing Clause	RFP Modified Clause
1.	5	Section 1 KEY INFORMATION **Last Date and Time for submission of Bids**	27/03/2026 at 3:00 PM	08/04/2026 at 3:00 PM
2.	5	Section 1 KEY INFORMATION **Date and Time of Opening of Bids**	27/03/2026 at 3:30 PM	08/04/2026 at 3:30 PM

Punjab & Sind Bank
(A Govt. of India Undertaking)
Where service is a way of life

Addendum – 01

S. No	Page No.	RFP Section No.	RFP Existing Clause	RFP Modified Clause
3.	25	Section 8 EVALUATION CRITERIA, 8.1 Eligibility evaluation requirements Clause 3	The bidder should be currently empaneled by CERT-In as Information Security Auditing Organizations	The bidder should be currently empaneled by CERT-In as on date of bid submission
4.	25	Section 8 EVALUATION CRITERIA, 8.1 Eligibility evaluation requirements Clause 4	The bidder should have a minimum turnover of INR 40 crore per annum in India for each of the past 3 financial years (i.e. 2022 23, 2023-24 & 2024-25) along with positive net worth.	The bidder should have a minimum average turnover of INR 30 Crore in India during the past 3 financial years (i.e. 2022 23, 2023-24 & 2024-25) along with positive net worth.
5.	25	Section 8 EVALUATION CRITERIA, 8.1 Eligibility evaluation requirements Clause 5	The Bidder should have at least 50 certified resources on its payroll, such as CEH, OSCP, CISA, CISSP, CompTIA Security+, CHFI, ISO/IEC 27001 LA/LI, eJPT or equivalent certifications.	The Bidder should have at least 25 certified resources on its payroll, such as CEH, OSCP, CISA, CISSP, CompTIA Security+, CHFI, ISO/IEC 27001 LA/LI, eJPT or equivalent certifications.
6.	25-26	Section 8 EVALUATION CRITERIA, 8.1 Eligibility evaluation requirements Clause 6	The Bidder must have experience and expertise in completing at least 1 assignment in listed each of the below service categories for a Scheduled Commercial Bank in India with minimum 1000 branches and value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP List of Service Categories: 1. Cyber Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cyber drill 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC Note: The experience for these service categories may be demonstrated through assignments carried out for one or more different clients; however, at least one	The Bidder must have experience with successful completion of at least 1 assignment in each of the listed below service categories for BFSI (including Regulators/Statutory body, Cert-In, NPCI, NCIIPC) in India during the last 5 years, as on the date of publication of the RFP List of Service Categories: 1. Cyber Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cyber drill 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC

			completed assignment is required for each category	Note: The experience for these service categories may be demonstrated through assignments carried out for one or more different clients; however, at least one completed assignment is required for each category
6.	26	Section 8 EVALUATION CRITERIA, 8.1 Eligibility evaluation requirements Clause 7	The Bidder must have experience and expertise in completing at least 1 assignment in cyber/digital forensic investigation for a BFSI in India with minimum 1000 branches during the last 3 years, as of the date of publication of the RFP Service Categories: 1. Cyber/Digital Forensic Investigation	The Bidder must have experience with successful completion of at least 1 assignment in each of the listed below service categories for BFSI (including Regulators/Statutory body, Cert-In, NPCI, NCIIPC) in India during the last 5 years, as on the date of publication of the RFP Service Categories: 1. Cyber/Digital Forensic Investigation
7.	25-26	Section 8 EVALUATION CRITERIA, 8.1 Eligibility evaluation requirements Clause 6 and Clause 7, Column "Documentary Proof"	1. PO/Contract Copy 2. Client Credential/client Confirmation	1. PO/Contract Copy 2. Client Credential / Client Confirmation / Client Email Confirmation/ Invoice of the milestone completion (along with Client confirmation Email and CA Certificate confirming the payment being received for the said milestone All submitted documents must clearly demonstrate the services provided and the successful completion/stage of the milestone. For client email confirmation- Name, Designation, Valid contact number of the personnel should be visible in the email

Punjab & Sind Bank
(A Govt. of India Undertaking)
Where service is a way of life

Addendum – 01

8.	27	Section 8 EVALUATION CRITERIA, 8.1 Eligibility evaluation requirements Clause 13	To avoid conflict of interest the successful bidder or its subsidiary or its associate or sister company or its holding company should not be the NextGEN SOC /IT Security /SOC vendor/Consultant of the bank under the existing or new contract	To avoid conflict of interest the successful bidder or its subsidiary or its associate or sister company or its holding company should not be the existing NextGEN SOC /IT Security /SOC vendor/Consultant of the bank as on the date of publication of the RFP. For the purposes of this RFP, "Consultant" here refers to the firm which is managing the current RFP (BID NO: PSB/ HO-CISO CELL/2026/SERVICES RFP DATED 20/02/2025) process.
9.	28	Section 8 EVALUATION CRITERIA, 8.2 Technical evaluation requirements Clause 4	The bidders should score minimum overall 80% marks in total for further selection process. The Bidders who do not qualify the section wise cut-off or total cut off will be dropped at this stage	Bidders scoring at least the minimum score of 70 marks or more will be declared technically qualified. The bidders scoring less than 70 marks (cut-off score) out of 100 marks in the technical evaluation criteria defined in the below table shall not be considered for further selection process and their offers will be dropped at this stage.
10.	28	Section 8 EVALUATION CRITERIA, 8.2 Technical evaluation requirements Clause 1	The bidder should have a minimum turnover per annum in India for each of the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth 1. Point 1: >40 Crores and <=60 Crore 2. Point 1: >60 Crores and <=80 Crore 3. Point 1: >80 Crores Marks 1. Point 1 = 6 Marks 2. Point 2 = 8 Marks 3. Point 3 = 10 Marks	Clause Stands deleted

Punjab & Sind Bank
(A Govt. of India Undertaking)
Where service is a way of life

Addendum – 01

			Maximum Marks – 10 Marks	
11.	28 – 29	Section 8 EVALUATION CRITERIA, 8.2 Technical evaluation requirements Clause 2	The Bidder must have experience and expertise in completing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India having not less than 1000 branches during the last 3 years, as on the date of publication of the RFP Service Categories: 1. Cyber Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cyber drill 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC Marks Number of assignments per service: 1. 2 assignments → 3 Marks 2. 3 assignments → 4 Marks 3. 4 assignments → 5 marks 4. 5 assignments → 6 marks Maximum marks – 36 marks Scoring will be conducted for each service individually and then consolidated to determine the highest overall score.	The Bidder must have experience and expertise in completing assignment in each of the service categories listed below during the last 5 years, as on the date of publication of the RFP. Service Categories: 1. Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cyber Drill Services 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC Note: A maximum of **FIVE (5) assignments** per service category shall be considered for evaluation and scoring purposes. **Marks** For each service category, marks shall be awarded based on the nature and status of the assignment, as detailed below: A) Scheduled Commercial Bank (including Regulators / Statutory body, Cert-In, NPCI, NCIIPC) in India) **Completed assignment – 3 Marks Per assignment**

				B) BFSI (Registered with Regulators RBI, SEBI, IRDAI, PFRDA) **Completed assignment – 2.5 Marks Per assignment** **Maximum Marks – 75 Marks**
12.	29	Section 8 EVALUATION CRITERIA, 8.2 Technical evaluation requirements Clause 3	The Bidder must have experience and expertise in completing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India of value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP Service Categories: 1. Cyber Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cyber drill 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC Marks Number of assignments per service: 1. 2 assignments → 3 Marks 2. 3 assignments → 4 Marks 3. 4 assignments → 5 marks 4. 5 assignments → 6 marks Maximum marks – 36 marks	Clause stands deleted

			Scoring will be conducted for each service individually and then consolidated to determine the highest overall score.	
13.	29-30	Section 8 EVALUATION CRITERIA, 8.2 Technical evaluation requirements Clause 4	The Bidder must have experience and expertise in completing assignment in cyber/digital forensic investigation for a BFSI not less than 1000 Branches in India during the last 3 years, as of the date of publication of the RFP. Service Categories: 1. Cyber/Digital Forensic Investigations Marks BFSI service marks depend on number of assignments per service: 1. 2 assignments → 7 Marks 2. 3 assignments → 10 Marks 3. 4 assignments → 14 Marks 4. 5 assignments → 18 marks Maximum marks – 18 marks	The Bidder must have experience and expertise in completing assignment in each of the service categories listed below during the last 5 years, as on the date of publication of the RFP Service Categories: 1. Cyber/Digital Forensic Investigations Note: A maximum of **FIVE (5) assignments** per service category shall be considered for evaluation and scoring purposes. **Marks** For each service category, marks shall be awarded based on the nature and status of the assignment, as detailed below: A) Scheduled Commercial Bank (including Regulators / Statutory body, Cert-In, NPCI, NCIIPC) in India) **Completed assignment – 5 Marks Per assignment** B) BFSI (Registered with Regulators RBI, SEBI, IRDAI, PFRDA) **Completed assignment – 4.5 Marks Per assignment** **Maximum Marks – 25 Marks**

Punjab & Sind Bank **Addendum – 01**
(A Govt. of India Undertaking)
Where service is a way of life

14.	33	Section 10.1 Service Delivery & Reporting SLA Services – Risk Assessment	Non- Critical Applications	Non- Critical Applications – 20
15.	32	Section 10 : SERVICE LEVEL & PENALITIES	Additional Clause	**The success criteria (MTTD, MTTR, regulatory reporting timelines)** **Mean time to Detect-** Critical Incidents - 45 Min Low Incident - 2 Hours **Mean time to recover** Critical Incident - 8 Hours. However, Incident should be contained within 2 Hours Low Incident - 48 Hours **Reporting:** Critical incident- 12 Hours Low Incident - 36 Hours
16.	37	Section 12.14 Liquidated Damages	The Bank will consider the inability of the bidder to deliver or install the equipment & provide the services required within the specified time limit as a breach of contract and would entail the payment of Liquidated Damages on the part of the bidder. The liquidated damages represent an estimate of the loss or damage that the Bank may have suffered due to delay in performance of the obligations (relating to delivery, installation, operationalization, implementation, training, acceptance, maintenance , ATS/AMC etc. of the proposed solution/services) by the bidder.	The Bank will consider the inability of the bidder to deliver or install the equipment & provide the services required within the specified time limit as a breach of contract and would entail the payment of Liquidated Damages on the part of the bidder. The liquidated damages represent an estimate of the loss or damage that the Bank may have suffered due to delay in performance of the obligations (relating to delivery, installation, operationalization, implementation, training, acceptance, maintenance , ATS/AMC etc. of the proposed solution/services) by the bidder.

			Installation will be treated as incomplete in one / all the following situations: a. Non-delivery of any component or other services mentioned in the order b. Non-delivery of supporting documentation c. Delivery / availability, but no installation of the components and/or software d. No integration/ Incomplete Integration e. Non-Completion of Transition within suggested timeline f. System operational, but not as per SLA, Timelines and scope of the RFP If the bidder fails to deliver any or all of the products and/or systems and/or services solutions within the time period(s) specified in the Delivery Schedule or installation, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 0.5 percent per week or part thereof of Contract Price subject to maximum deduction of 10% of the total contract value, until actual delivery, installation or performance as per related clauses mentioned in RFP. Once the maximum deduction is reached, the Bank may consider termination of the Contract at its discretion. In the event of Bank agreeing to extend the date of delivery at the request of successful	Installation/Services will be treated as incomplete in one / all the following situations: a. Non-delivery of any component or other services mentioned in the order b. Non-delivery of supporting documentation c. Delivery / availability, but no installation of the components and/or software d. No integration/ Incomplete Integration e. Non-Completion of Transition within suggested timeline f. System operational, but not as per SLA, Timelines and scope of the RFP If the bidder fails to deliver any or all of the products and/or systems and/or services solutions within the time period(s) specified in the Delivery Schedule or installation, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 0.5 percent per week or part thereof of Contract Price subject to maximum deduction of 10% of the total contract value, until actual delivery, installation or performance as per related clauses mentioned in RFP. Once the maximum deduction is reached, the Bank may consider termination of the Contract at its discretion.

			bidder(s), it is a condition precedent that the validity of Bank guarantee shall be extended by further period as required by Bank immediately. Failure to do so will be treated as breach of contract. If Successful bidder fails to deliver any or all of the Service(s) or perform the Services within the time period(s) specified in the RFP/Contract / Agreement, BANK shall, without prejudice to its other rights and remedies under and in accordance with the RFP/Contract / Agreement, levy Liquidated Damages (LD) from payments, which are due to the Successful bidder. For calculation of LD: The contract price for calculation of LD is TCO. • The overall LD during certification/sustenance will be to a maximum of 25% of the contract value. • LD for delay in Commencement/completion of services for each week of delay beyond the scheduled Commencement/completion date or part thereof will be a sum equivalent to 2% of unperformed services per week. In case of undue delay beyond a period of 15 days after attaining the maximum penalty of 10% of total project cost, Bank may consider termination of the contract or purchase order.	In the event of Bank agreeing to extend the date of delivery at the request of successful bidder(s), it is a condition precedent that the validity of Bank guarantee shall be extended by further period as required by Bank immediately. Failure to do so will be treated as breach of contract.

			• Part of week will be considered as full week. • Any delay by the bidder in performance of its delivery obligations shall render the bidder liable to the imposition of liquidation damages, unless extension of time is agreed upon without application of liquidation damages. • The liquidated damages shall be deducted/recovered by the Bank from any money due or becoming due to the Bidder under this Purchase Contract or may be recovered by invoking of Bank Guarantees otherwise from Bidder or from any other amount payable to the Bidder in respect of other orders. Levying Liquidated damages is without prejudice to the Bank's right to levy any other penalty where provided for under the contract. • Any such recovery or liquidated damages shall not in any way relieve the Successful bidder from any of its obligations to complete the works / service(s) or from any other obligations and liabilities under the Contract/Agreement/Purchase Order. • Bank reserves the right to condone the delay, if it is not attributable to the Successful bidder.	

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
1	17	6 - Scope of Work	Overall Scope	Do we have to conduct VA ? Are all devices accessible from 1 centralized location	Please be guided by the RFP, VAPT is not to be performed by the bidder
2	18	6.1 Risk Assessment	Brief Scope of Work	Kindly confirm whether the Bank currently maintains an active ISO/IEC 27001 certification. Additionally, kindly confirm whether relevant certification documents (e.g., certificate, Statement of Applicability, and latest audit reports) can be shared to support the gap analysis.	Yes, bank has ISO/IEC 27001 certification. If required, documents will be shared with successful bidder
3	18	6.1 Risk Assessment	Brief Scope of Work	Kindly confirm the number of non-critical applications to be covered under annual risk assessments.	The count of application is in the Bill of material. i.e 20 Applications.
4	18	6.1 Risk Assessment	Brief Scope of Work	Kindly provide the approximate number of third-party vendors expected to be covered annually under this scope.	The bank has identified a total of 57 applications for risk assessment. These assessments are to be conducted for their respective vendors. In some cases, a single vendor may provide multiple applications, and the scope also includes in-house applications. The approximate number of third-party vendors involved is 40
5	18	6.1 Risk Assessment	Brief Scope of Work	Kindly provide the count and location details of Data Centre (DC), Disaster Recovery (DR), and Near Disaster Recovery (NDR) sites to be assessed.	DC- Navi Mumbai - Qty 1 DR- Noida - Qty 1 NDR- Navi Mumbai - Qty 1
6	18	6.2 Forensic Investigation	Point 6 Ensure proper chain of custody is maintained to protect integrity and all evidence recovery and collection methods are conducted, managed, and achieved in a manner consistent to maintain preservation and protection of data and evidence in its original form such that it may be admissible in the court of Law.	Kindly confirm whether court-admissible forensic reports are required for all investigations or only for specific cases.	The Activity is to be performed for all investigation as mentioned in the requirement
7	19	6.4	Point 5 Backup and restoration readiness assessment, covering offsite, offline, immutable, and air-gapped backups; ransomware-proof storage; and verification of restore procedures	Kindly confirm the backup solution OEM currently in use and whether immutable backups are already implemented.	Multiple backup solution are in place like Commvault, Veritas, Dell etc.
8	19	6.3 Configuration Review	Point 2. Assessment of operating system hardening for Windows, Linux, and other platforms, including user rights, password policies, services, patch levels, and audit settings	Approximate number of Windows/Linux servers in scope?	Details shall be shared with the successful bidder
9	19	6.3 Configuration Review	Point 3. Configuration review of SIEM, SOAR, UEBA, firewalls, other security devices and network devices including rule-base evaluation, access control lists (ACLs), NAT policies, VPN settings, and logging.	Approximate number of SIEM, SOAR, UEBA, firewalls, other security devices and network devices	Please refer BOM. The count of devices i.e 10
10	19	6.3 Configuration Review	Point 4. Security configuration review of endpoints, including antivirus/EDR, patching, encryption, and device hardening.	Total number of endpoints (servers + desktops + laptops) under review?	Details shall be shared with the successful bidder
11	19	6.3 Configuration Review	Ponit 5. Database security assessment covering authentication, privileges, schema protection, audit logs, and data encryption	Approximate number of Database in Scope	Details shall be shared with the successful bidder
12	19	6.3 Configuration Review	Point 6. Review of application server configurations (Web/App servers) including SSL/TLS settings, session management, and directory permissions	Approximate number of web servers in Scope	Details shall be shared with the successful bidder
13	19	6.3 Configuration Review	Point 7. Validation of identity and access management (IAM) settings, including privileged access controls, role-based access, MFA enforcement, and user lifecycle processes.	Kindly confirm IAM/PAM OEM and number of privileged accounts to be assessed.	Details shall be shared with the successful bidder
14	19	6.3 Configuration Review	Point 8. Examination of security logging and monitoring configuration, including log retention, SIEM integration, and alert rules	Whether log source validation includes branch/ATM systems or only DC/DR?	It is only DC/DR/NDR
15	19	6.3 Configuration Review	Point 13. Preparation of document all existing OS, proprietary OS, addition of OS as updated and Annual review of all document.	Whether we must prepare fresh baseline documents or update existing ones.	As a part of the Scope requirement following is to be performed: 1. One time -Fresh creation & preparation 2. Regular- Update/Augment the document as per the frequency defined in the RFP
16	19	6.3 Configuration Review	Point 13. Preparation of document all existing OS, proprietary OS, addition of OS as updated and Annual review of all document.	How many OS platforms (including proprietary OS) are currently deployed?	The count of OS platform is in the Bill of material. i.e 50
17	20	6.5 Cybersecurity Awareness & Content Development	Cybersecurity awareness is a critical component of a bank's overall security posture. It focuses on educating employees and stakeholders about threats, vulnerabilities, and best practices to safeguard digital assets. As humans are often the weakest link in security, a well-structured awareness program strengthens the first line of defense against cyberattacks such as phishing, ransomware, social engineering, and insider threats	**Target Audience Coverage:** Kindly provide the approximate number of: • Employees • Vendors • Customers to be covered under the awareness program for each session. **Number and Frequency of Sessions:** • Please confirm the total number of sessions to be conducted in a year. • Kindly specify the required frequency (e.g., monthly, quarterly, half-yearly, etc.). **Mode of Delivery:** • Whether the sessions are to be conducted onsite, remotely (virtual), or in hybrid mode? • If onsite, kindly confirm the location(s) where the sessions are expected to be conducted.	Target Audience Coverage for session is Employess and vendors Kindly refer BOM and Annexure 15. Online Session will be conducted

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
18	20	6.5 Cybersecurity Awareness & Content Development	Point 7 Design and execution of IVR-based cyber security awareness messages for employees and stakeholders, including scripting, voice recording, and scheduled call campaigns. Messages shall focus on current cyber threats, safe digital practices, and regulatory advisories, with periodic updates aligned to emerging risks.	Kindly confirm the expected campaign frequency along with the approximate call volumes per campaign.	Bidder to provide the material to Bank. Rest of the details will be shared with successful bidder
19	20	6.6 Cyber Drill Services	Scope of work point 1 to 12	Kindly confirm the number of cyber drills to be conducted annually during the contract period.	Please be guided by the RFP, Refer Section 13.15
20	21	6.6 Cyber Drill Services	Point 4 Live or Controlled Technical Simulation (depending on bank's approval) to test SOC alerting, threat detection, and response capabilities	Whether live simulations in production environments are permitted or if only controlled simulations/tabletop exercises are expected.	Bidder to plan for both the simulations 1. Controlled Simulation in limited environment 2. Controlled Simaltion in Live Environment, post bank approval
21	21	6.7.1 Network architecture, segmentation, and data flow analysis	Network architecture, segmentation, and data flow analysis(Overall Scope)	Total number of Data Centers and DR sites in scope?	DC- Navi Mumbai - Qty 1 DR- Noida - Qty 1 NDR- Navi Mumbai - Qty 1
22	21	6.7.1 Network architecture, segmentation, and data flow analysis	Network architecture, segmentation, and data flow analysis(Overall Scope)	Approximate number of branches and ATMs to be covered?	the activity is to be performed for DC, DR & NDR
23	21	6.7.1 Network architecture, segmentation, and data flow analysis	Point 7. Configuration review of network and security devices including Firewall, IPS, IDS, Routers, Switches, etc	Total Number of network and security devices including Firewall, IPS, IDS, Routers, Switches, etc	Please refer section13.15, annexure 15
24	21	6.7.1 Network architecture, segmentation, and data flow analysis	Point 8. Rule based review of firewall and IPS	Total Number of firewall and IPS and total number of rules in each firewall	Details shall be shared with the successful bidder
25	21	6.7.1 Network architecture, segmentation, and data flow analysis	Point 1: Assess the placement and configuration of firewalls, IPS/IDS, WAF, load balancers, and DDoS protection devices	Total number of firewalls, IPS/IDS, WAF, load balancers, and DDoS protection devices in scope?	Details shall be shared with the successful bidder
26	22	6.7 Information Security Testing Services	Scope of Work from Point nos 1 to 12	Kindly confirm the total number of applications to be reviewed under the application and database security design scope.	Critical - 37 and Non Critical - 20 . As defined in BOM and Annexure 15
27	22	6.7 Information Security Testing Services	Scope of Work from Point nos 1 to 4	Kindly provide the total number of cloud environments in scope (e.g., AWS, Azure, etc.).	The bank is currently in the process of deploying a private cloud environment, while adoption of public cloud services is planned for a future phase.
28	22	6.7 Information Security Testing Services	Scope of Work from Point nos 1 to 4	Kindly confirm whether cloud configurations are centrally managed or distributed across multiple teams/business units.	The bank is currently in the process of deploying a private cloud environment, while adoption of public cloud services is planned for a future phase.
29	22	6.7 Information Security Testing Services	Scope of Work from Point nos 1 to 4	Kindly confirm the estimated number of cloud-hosted applications, APIs, and web services included within the assessment scope.	The bank is currently in the process of deploying a private cloud environment, while adoption of public cloud services is planned for a future phase.
30	22	Application and database security design	Point 2. Assess secure coding practices and adherence to OWASP Top 10 and SANS guidelines.	Is source code review in scope	The objective is to identify and address security vulnerabilities efficiently. The Bank requires assessment of secure coding practices and adherence to OWASP Top 10 and SANS guidelines for identifying potential security gaps in the application and databases. The scope is limited to security assessment
31	22	Application and database security design	Point 2. Assess secure coding practices and adherence to OWASP Top 10 and SANS guidelines.	Do we have to conduct web application security testing? If Yes, Total number of application count and size of application is required? Input fields 0-100 : Small Input fields 100-500: Medium Input fields more than 500: Large	The Bank is currently in the process of procuring an Application Security Testing Tool
32	22	Application and database security design	Point 4. Analyze API security, input validation, and encryption of data in transit	Approximate number of APIs to be assessed?	250 Public facing APIs
33	22	Application Security	API Security Assessment(Overall Scope)	Approximate number of APIs to be assessed?	250 Public facing APIs
34	22	Application Security	API Security Assessment(Overall Scope)	API count in clause 6.7.4.4 and 6.7.8 are same or different	250 Public facing APIs
35	23	6.7 Information Security Testing Services	Scope of Work from Point nos 1 to 10	Kindly confirm the number of tabletop exercises expected during the engagement (single vs. multiple sessions).	Please refer BOM
36	23	6.7 Information Security Testing Services	Scope of Work from Point nos 1 to 10	Kindly confirm whether separate sessions are required for Blue Team and Grey Team simulations.	Depending upon the session and requirement, bidder is required to perform the simulations, it may be organized as combined activity or as separate, same shall be defined and agreed during the requirement gathering session
37	24	8 EVALUATION CRITERIA	Point 4- he bidder should have a minimum turnover of INR 40 crore per annum in India for each of the past 3 financial years (i.e. 2022 - 23, 2023-24 & 2024-25) along with positive net worth.	The current stipulation of Rs. 40 Crores annual turnover for each of the last three financial years appears to be on the higher side and may be restrictive in nature. Such a high threshold could significantly limit participation, thereby reducing fair competition among otherwise qualified and experienced bidders. Hence, we recommend that the Annual turnover for each year of the bidder for the last 3 financial years should be Rs. 10 Crores instead of Rs. 40 Crores. We request your kind consideration of the above suggestion in the interest of promoting healthy competition and ensuring wider vendor participation.	Please refer addendum for revised clause
38	24	8 EVALUATION CRITERIA	Point 5 - The Bidder should have at least 50 certified resources on its payroll, such as CEH, OSCP, CISA, CISSP, CompTIA Security+, CHFI, ISO/IEC 27001 LA/LI, eJPT or equivalent certifications.	Whether the bidder is required to submit any one of the specified certificates, or each and every certificate mentioned in the clause? We request you to please confirm the exact requirement to ensure proper compliance with the tender conditions.	The Requirement is self explanatory, the bidder should have on their payroll the required quantity of certified resources with either of the certifications mentioned in the clause

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
39	24	11	Level 1 (L1) a. Experience of above 2 years b. Educational Qualifications: B.Tech/B.E/BCA/MCA or any other relevant graduation c. Minimum one of below Mandatory Certifications: CEH/LPT/CCNA/ ISO 27001 LA/LI/ITIL/relevant service certification or Certifications as per Level 2 or Level 3 d. At least 1 BFSI experience of conducting similar services	Please delete the LPT for L1 resource	Please be guided by the RFP
40	24	11	B) Level 2 (L2) a. Experience of above 5 years b. Educational Qualifications: B.Tech/B.E/BCA/MCA or any other relevant graduation c. At least one of the Mandatory certifications below: CISA / CISM / CISSP / OSCP / OSCE/relevant service certification d. At least 2 BFSI experience of conducting similar services	Please add CEH as well	Please be guided by the RFP, Bidder can propose the resource with relevant certification as required for performing the services
41	24	11	C) Level 3 (L3) a. Experience of above 7 years b. Educational Qualifications: B.Tech/B.E/BCA/MCA or any other relevant graduation c. At least Two (2) of the Mandatory certifications below: CISA / CISM / CISSP / OSCP/ OSCE/relevant service certification d. At least 3 BFSI experience of conducting similar services	Please Add CHFI , CPENT & LPT	Please be guided by the RFP, Bidder can propose the resource with relevant certification as required for performing the services
42	24	8 EVALUATION CRITERIA	Point6 - the Bidder must have experience and expertise in completing at least 1 assignment in listed each of the below service categories for a Scheduled Commercial Bank in India with minimum 1000 branches and value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP. List of Service Categories: 1. Cyber Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cyber drill 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC Note: The experience for these service categories may be demonstrated through assignments carried out for one or more different clients; however, at least one completed assignment is required for each category	With reference to the tender conditions, we would like to submit the following requests for your kind consideration: **I. Work Order Requirement & Activity Criteria** If submission of work orders covering the complete list of activities mentioned is made mandatory, the eligibility criteria will become highly restrictive. As a result, many CERT-In empanelled vendors may be unable to participate despite having relevant expertise. Further, as per by the Reserve Bank of India (RBI), statutory/IT audit firms are required to be rotated and should not continue indefinitely. In line with fair competition and broader participation, we request suggest that bidders be required to demonstrate experience & work order in any 3 out of the 5 listed activities, instead of all 5 activities and also in page number 29 clause 8.2 Technical evaluation requirements point 3 there are 6 category. Please confirm This will ensure adequate competition while maintaining quality standards. **II. Request for Removal of INR 40 Lakhs Clause** We request you to kindly reconsider the clause stating: "The Bidder must have experience and expertise in completing at least one assignment in each of the service categories listed below for a Scheduled Commercial Bank in India of value not less than INR 40 Lakhs during the last 3 years." While we have handled purchase orders (POs) of significantly higher values, not every PO individually covers all the specified service categories. This clause may therefore unintentionally disqualify competent bidders who possess substantial experience but across	Please refer addendum for revised clause
43	27	8 EVALUATION CRITERIA	Point 11 - Integrity Pact document on 100 Rs Stamp paper, duly signed, stamped and notarized by the authorized signatory.	Please confirm do we need to submit along with the bid	Integrity pact is to be submitted on Stamp Paper along with the bid
44	27	8 EVALUATION CRITERIA	Point 12 - Non-Disclosure Agreement document on 100 Rs Stamp paper, duly signed, stamped and notarized by the authorized signatory.	Please confirm do we need to submit along with the bid	NDA is to be submitted on Stamp Paper along with the bid

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
45	28	8.2	Sr. Nos 1 -The bidder should have a minimum turnover per annum in India for each of the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth 1. Point 1: >40 Crores and <=60 Crore 2. Point 1: >60 Crores and <=80 Crore 3. Point 1: >80 Crores 1. Point 1 = 6 Marks 2. Point 2 = 8 Marks 3. Point 3 = 10 Marks Maximum Marks – 10 Marks	1. Point 1: >40 Crores and <=60 Crore 2. Point 1: >60 Crores and <=80 Crore 3. Point 1: >80 Crores The current stipulation of Rs. 80 Crores annual turnover for each of the last three financial years appears to be on the higher side and may be restrictive in nature. Such a high threshold could significantly limit participation, thereby reducing fair competition among otherwise qualified and experienced bidders. Hence, we recommend that the Annual turnover for each year of the bidder for the last 3 financial years should be Rs. 10 Crores instead of Rs. 40 Crores. We request your kind consideration of the above suggestion in the interest of promoting healthy competition and ensuring wider vendor participation. We request to propose following the bidder should have a minimum turnover per annum in India for each of the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth 1. Point 1: >5 Crores and <=10 Crore 2. Point 1: >10 Crores and <=15 Crore 3. Point 1: >20 Crores	Please refer addendum for revised clause
46	28	8.2	Point 2 The Bidder must have experience and expertise in completing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India having not less than 1000 branches during the last 3 years, as on the date of publication of the RFP Service Categories: 1. Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cybersecurity Awareness & Content Development 5. Cyber Drill Services 6. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC Number of assignments per service: 1. 2 assignments → 3 Marks 2. 3 assignments → 4 Marks 3. 4 assignments → 5 marks 4. 5 assignments → 6 marks Maximum marks – 36 marks Scoring will be conducted for each service individually and then consolidated to determine the highest overall score	With reference to the tender conditions, we would like to submit the following requests for your kind consideration: **I. Work Order Requirement & Activity Criteria** If submission of work orders covering the complete list of activities mentioned is made mandatory, the eligibility criteria will become highly restrictive. As a result, many CERT-In empanelled vendors may be unable to participate despite having relevant expertise. Further, as per by the Reserve Bank of India (RBI), statutory/IT audit firms are required to be rotated and should not continue indefinitely. In line with fair competition and broader participation, we request suggest that bidders be required to demonstrate experience & work order in any 3 out of the 5 listed activities, instead of all 5 activities and also in page number 29 clause 8.2 Technical evaluation requirements point 3 there are 6 category. Please confirm This will ensure adequate competition while maintaining quality standards. **II. Request for Removal of INR 40 Lakhs Clause** We request you to kindly reconsider the clause stating: "The Bidder must have experience and expertise in completing at least one assignment in each of the service categories listed below for a Scheduled Commercial Bank in India of value not less than INR 40 Lakhs during the last 3 years." While we have handled purchase orders (POs) of significantly higher values, not every PO individually covers all the specified service categories. This clause may therefore unintentionally disqualify competent bidders who possess substantial experience but across different assignments	Please refer addendum for revised clause
47	29	8.2	Point 4 - The Bidder must have experience and expertise in completing assignment in cyber/digital forensic investigation for a BFSI not less than 1000 Branches in India during the last 3 years, as of the date of publication of the RFP. Service Categories: 1. Cyber/Digital Forensic Investigations BFSI service marks depend on number of assignments per service: 1. 2 assignments → 7 Marks 2. 3 assignments → 10 Marks 3. 4 assignments → 14 Marks 4. 5 assignments → 18 marks Maximum marks – 18 marks	The requirement to provide work orders for up to five (5) assignments for BFSI organizations with more than 1000 branches appears to be highly restrictive in nature. Such large-scale forensic assignments are limited in number and opportunity, and not all capable and technically competent firms get multiple opportunities of this scale, despite possessing the necessary expertise, skilled resources, and relevant certifications. This condition may significantly limit participation and reduce fair competition among experienced and qualified bidders. In this regard, we request that the clause be modified to: Require submission of minimum one (1) eligible work order meeting the stated criteria, instead of five assignments; and Rationalize the marking structure accordingly to ensure broader participation while maintaining quality standards. We believe this modification will promote healthy competition and allow capable organizations to participate, without compromising the objective and quality expectations of the RFP. We request your kind consideration of the above recommendation.	Please refer addendum for revised clause
48	44- 73	ANNEXURES	ANNEXURES	Please provide the work copy of the annexure	Please be guided by the RFP
49	Page 5 of 73	KEY INFORMATION	Last Date and Time for submission of Bids: 13/03/2026 at 3:00 PM	We kindly request the Bank to extend the timeline till 27 March 2026 allowing us with an adequate opportunity to complete our evaluation and ensure there is no conflict of interest with respect to Clauses 12 and 13 of the "Eligibility Evaluation Requirements."	Please refer addendum for revised clause

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
50	Page 5 of 73	KEY INFORMATION	Rs. 51,00,000/- (INR Fifty-One Lakh Only)	Given that the Estimated Bid Value is INR 16,96,00,000.00, we kindly request the Bank to consider setting the EMD amount at 2% of the bid value, i.e., INR 33,80,000.00.	Please be guided by the RFP
51	Page 25 of 73	EVALUATION CRITERIA	The bidder should have a minimum turnover of INR 40 crore per annum in India for each of the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth.	Given the Estimated Bid Value is INR 16,96,00,000.00, we kindly request the Bank to set the turnover limit to 100 Crore per annum in India for each of the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth.	Please refer addendum for revised clause
52	Page 26 of 73	EVALUATION CRITERIA	The Bidder must have experience and expertise in completing at least 1 assignment in listed each of the below service categories for a Scheduled Commercial Bank in India with minimum 1000 branches and value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP List of Service Categories: 1. Cyber Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cyber drill 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC Note: The experience for these service categories may be demonstrated through assignments carried out for one or more different clients; however, at least one completed assignment is required for each category	We kindly request the Bank to include the following statement at the end of the relevant RFP clause: "The experience in the aforesaid areas should be derived from either one or multiple PO/WO/ELs within a single financial year from a single Scheduled Commercial Bank in India having a minimum of 1,000 branches."	Please refer addendum for revised clause
53	Page 26 of 73	EVALUATION CRITERIA	The Bidder must have experience and expertise in completing at least 1 assignment in cyber/digital forensic investigation for a BFSI in India with minimum 1000 branches during the last 3 years, as of the date of publication of the RFP Service Categories: 1. Cyber/Digital Forensic Investigation	We kindly request the Bank to amend the clause as follows: The Bidder must have experience and expertise in completing at least 1 assignment in cyber/digital forensic investigation or digital forensic readiness assessment or malware analysis for a BFSI in India with minimum 1000 branches during the last 3 years, as of the date of publication of the RFP Service Categories: 1. Cyber/Digital Forensic Investigation	Please refer addendum for the revised clause
54	Page 28 of 73	EVALUATION CRITERIA	The bidder should have a minimum turnover per annum in India for each of the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth 1. Point 1: >40 Crores and <=60 Crore 2. Point 1: >60 Crores and <=80 Crore 3. Point 1: >80 Crores	We kindly request the Bank to amend the clause as follows: The bidder should have a minimum turnover per annum in India for each of the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth 1. Point 1: >40 Crores and <=60 Crore 2. Point 1: >60 Crores and <=100 Crore 3. Point 1: >100 Crores	Please refer addendum for revised clause
55	Page 28 of 73	EVALUATION CRITERIA	The Bidder must have experience and expertise in completing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India having not less than 1000 branches during the last 3 years, as on the date of publication of the RFP	May we kindly request the Bank to confirm whether marks will be allocated based on PO values of INR 40 lakhs and above or any experience and expertise irrespective of value. For example, if a bidder has executed two projects with PO values exceeding INR 40 lakhs each, will the bidder be awarded 3 marks accordingly?	Please refer addendum for revised clause
56	Page 28 of 73	EVALUATION CRITERIA	The Bidder must have experience and expertise in completing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India of value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP	If the above criterion refers to any value, we assume that this clause refers to PO/WO value of INR 40 lakhs. Kindly confirm.	Please refer addendum for the revised clause
57	Page 33 of 73	10 SERVICE LEVEL & PENALITIES	Non-Critical Application	May we kindly request the Bank to confirm the number of non-critical application	The count of application is in the Bill of material. i.e 20 Applications.
58	Page 33 of 73	10 SERVICE LEVEL & PENALITIES	Forensic Investigation	May we kindly request the Bank to confirm the if the additional payment would be prorate basis if digital forensic services goes beyond total 100 Man hours. Could you please confirm the indicative number of such incidents in last three years	The Number, 100, mentioned in the RFP is for TCO (Total cost of ownership) calcualtion purpose and per incident service value would be arrived based on per person hours rates (/pro-rata basis) provided in the BOM
59	Page 33 of 73	10 SERVICE LEVEL & PENALITIES	Cyber security Awareness Content Development	May we kindly request the Bank to confirm the if online awareness sessions will be imparted on Bank provided platform.	The bidder will use the WebEx portal for the meeting. If any additional platform is required, the bidder must account for it accordingly.
60	Page 18 of 73	6 Scope of Work	9. Third party Technology Risk & supply chain Risk Review.	May we kindly request the Bank to confirm the if the bidder is responsible to evaluate the Third party Technology Risk & supply chain Risk governance framework or vendor audit is included in the scope. If vendor audit is included, please provide us the number of vendor.	The bank has identified a total of 57 applications for risk assessment. These assessments are to be conducted for their respective vendors. In some cases, a single vendor may provide multiple applications, and the scope also includes in-house applications. The approximate number of third-party vendors involved is 40
61	Page 18 of 73	6 Scope of Work	Review of security configurations of servers, databases, network devices, cloud resources, and security appliances against industry best practices (CIS Benchmarks, NIST, RBI, ISO 27001).	Please provide us the number of: - Servers: - OS: - Databases: - Network devices ((Router, Switches, firewalls, IPS/IDS, WAF): - Cloud resources (Subscription/ license): - Security appliances: - End point:	Details shall be shared with the successful bidder

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
62	Page 18 of 73	6 Scope of Work	Preparation of document all existing OS, proprietary OS, addition of OS as updated and Annual review of all document.	Please confirm if preparation of Secure Configuration Document (SCD) or Minimum baseline security standard (MBSS) is the part of scope. If yes, please provide us the indicative number of SCD document to be prepared against each category of devices (e.g. Windows 2016, windows 2020, etc.)	Please be guided the RFP, requirement is explicit. refer section 13.15 of the RFP
63	Page 18 of 73	6 Scope of Work	6.7.8 API Security Assessment	Please provide us the number of API	250 Public facing APIs
64	18	Risk Assessment	Critical Business Process	What is the complete asset inventory (servers, endpoints, network devices, applications, databases) with quantities per category? How many business processes and critical information flows exist? How many third-party vendors integrate with Bank systems & what interfaces exist?	Please refer BOM/Annexure 15/ Any additional detaill will be shared with successful bidder
65	18	Risk Assessment	Technology understanding	What are the type of 37 critical applications and the count of non-critical apps requiring review?	Please refer BOM
66	18	Risk Assessment	Regulatory Requirement	What data types is bank handling (PII, PCI, financial) and where are they stored? What regulatory frameworks apply (RBI cybersecurity, ISO 27001, IT Act, PCI DSS)? Are there any major IT or digital transformation projects planned in the next 12 months?	Will be shared with successful bidder.All Government of India, RBI, Regulatory & statutory framework applicable to the bank shall be complied
67	18	Forensic Investigation	Volume and Frequency	What is the incident volume trend over the past 12–24 months (P1/P2/P3)? What is the Bank's log retention period, and which systems generate logs accessible for forensics?	Will be shared with successful bidder.All Government of India, RBI, Regulatory & statutory framework applicable to the bank shall be complied
68	18	Forensic Investigation	Digital Assets consideration	Please share if bank already has any existing forensics tool in place or does bidder needs to be provided as part of this RFP. Please share the list of devices (server/endpoint/mobile/network)?	The bank is currently not using any forensic tools. The bidder should factor this in as per the requirements.
69	18	Forensic Investigation	Scope of work	Is there an existing forensic lab, write-blockers, or imaging tools onsite? Who are the approval stakeholders for evidence handling (Legal, Compliance, CISO)?	The bank does not have any forensic lab. The approval hierarchy will be shared with the successful bidder.
70	18-19	Configuration and Rule Review	Volumetric	What is the breakdown of the ~3000 configurations (firewalls, routers, switches, servers, DBs, cloud, endpoints)? Also provide the number of devices for which configuration review needs to be done as part of scope?	Will be shared with successful bidder. Confuguration review is for 3000 devices
71	18-19	Configuration and Rule Review	Volume and access	What is the ruleset size per firewall/IPS/WAF device?	Details shall be shared with the successful bidder
72	18-19	Configuration and Rule Review	Volumetric	Please provide if bank has any policy review tool in place, if yes please provide the name of the tool.	The bank currently has a Firewall Analyzer tool in place; bidders are required to assess any additional tools needed and include them as part of their proposal.
73	18-19	Configuration and Rule Review	Volumetric	What OS versions (Windows/Linux/Solaris) exist and how many of each? How many privileged accounts and what % is MFA-enabled?	Details shall be shared with the successful bidder
74	19	Ransomware Readiness	Scope and Scale	What is the total endpoint estate, with breakdown by OS and user type?	Details shall be shared with the successful bidder
75	19	Ransomware Readiness	Environment	What is the EDR/XDR coverage % and policy configuration maturity?	Details shall be shared with the successful bidder
76	19	Ransomware Readiness	Architecture	What is the Bank's backup posture (RPO/RTO, immutability, air-gap, restore test success rate)?	The Bank's backup posture targets near-zero data loss with defined RPO/RTO aligned to criticality tiers (systems, based on their criticality, in minutes to a few hours), leveraging backups copies to protect against threats.
77	19	Ransomware Readiness	Network Segmentation	How is the network segmented (count of segments, ACL complexity)? What are the crown-jewel systems and their protection posture?	Details shall be shared with the successful bidder
78	20	Cybersecurity Awareness & Content Development	Volumetric	What is the total audience size (employees, vendors, customers) for awareness? And What formats are expected (videos, audios, quizzes, booklets, e-learning modules, presentations etc). Also help us with the frequency of Cybersecurity Awareness to be done?	Please refer Annexure 15 Online Session will be conducted
79	20	Cybersecurity Awareness & Content Development	Format	Which languages are required for training content? Does the Bank have an Learning Management System (LMS) and does it support Sharable Content Object Refence Model (SCORM)?	Training session/content will be in english. Bidder to share the detsils with Bank's SPOC
80	20	Cybersecurity Awareness & Content Development	Volumetric	What is the expected volume per month of content (videos, posters, quizzes)? What is the expected completion rate or compliance target?	2 - posters/month 2-Short videos/month 1- quiz/month 100% IS THE COMPLIANCE TARGET
81	20-21	Cyber Drill Services	Scope and Scale	Please confirm drills should be technical, tabletop, or hybrid? Also confirm on the scope and scale of cyber drills and participants, locations etc in scope?	The Drill should be Hybrid Location shall be Project office, DC, DR of the bank. List of pariticpants shall be shared before each drill
82	20-21	Cyber Drill Services	Volumetric	Which critical systems can be included in live simulation? Also what are the scenarios that is expected to be included as part of this engagement? And volume of expected scenarios?	Details shall be shared with the successful bidder
83	20-21	Cyber Drill Services	Access requirement	How many departments and roles participate in drills?	Details shall be shared with the successful bidder
84	20-21	Cyber Drill Services	Regulatory and compliance Requirement	What are the success criteria (MTTD, MTTR, regulatory reporting timelines)?	Please refer addendum for the revised clause
85	21-24	Information Security Testing Services	Baseline consideration	How many network devices exist by type (routers/firewalls/switches)?	Details shall be shared with the successful bidder
86	21-24	Information Security Testing Services	Volumetric	Please confirm on the total count of firewalls, IPS/IDS, WAF, load balancers, DDoS devices? Are these deployed in HA pairs or standalone? Are all devices integrated with SIEM/SOC?	Details shall be shared with the successful bidder
87	21-24	Information Security Testing Services	Volumetric	Please confirm on the total user count by type (employees, vendors, service accounts).	No. of users – 50 users for table top exercise
88	21-24	Information Security Testing Services	Volumetric	Please confirm on the number of privileged accounts and current PAM deployment? also MFA coverage % across user sets.	Details shall be shared with the successful bidder

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
89	21-24	Information Security Testing Services	Volumetric	Please confirm on the IAM/ PAM/ SSO tools in place. Also if any IGA governance tool in currently in place.	Yes Bank has such tools. Details will be shared with successful bidder
90	21-24	Information Security Testing Services	Volumetric	What is the Encryption coverage % (BitLocker, File Vault, others) also existing MDM/UEM tools deployed.	Details shall be shared with the successful bidder
91	21-24	Information Security Testing Services	Volumetric	Please confirm on the list of major cloud services (IaaS/PaaS/SaaS) in scope. Also help us with the number of assets in the existing cloud?	The bank is currently in the process of deploying a private cloud environment, while adoption of public cloud services is planned for a future phase.
92	21-24	Information Security Testing Services	Volumetric	Please confirm on the CSPM tool currently available at the Bank, provide the details of the tool.	Bank is in the process of procuring the CSPM tool, details shall be shared with the successful bidder
93	21-24	Information Security Testing Services	Volumetric	Please confirm on the existing HSM/KMS and number of encryption keys and rotation frequency (automated/ manual). If any automation tools is currently present please let us know.	Details shall be shared with the successful bidder
94	21-24	Information Security Testing Services	Volumetric	Please confirm on the total APIs in scope? Is there any existing security tools available?	250 Public facing APIs
95	21-24	Information Security Testing Services	Volumetric	Please share the number of existing playbooks to be reviewed?	Details shall be shared with the successful bidder
96	21-24	Information Security Testing Services	Volumetric	Please confirm on the reporting templates and artifacts required?	Details shall be shared with the successful bidder
97	21-24	Information Security Testing Services	Volumetric	What type of threat intelligence sources/subscriptions exist?	Details shall be shared with the successful bidder
98	21-24	Information Security Testing Services	Volumetric	Which regulatory frameworks are in scope (RBI, ISO, PCI)?	All Government of India, RBI, Regulatory & statutory framework applicable to the bank shall be complied
99	21-24	Information Security Testing Services	Volumetric	How many open audit findings/observations exist?	Bank undergoes Audit/Review by regulators at regulator interval during the contract period, details of which shall be shared with the successful bidder
100	24	Miscellaneous	Scope of work	What is PCI DSS scope (in-scope systems, CHD flow)? Are QSA assessment windows predefined?	bank operates only ATMs, the PCI DSS scope is limited to ATM systems, connected networks, and backend systems that process or transmit CHD. The activity is to be performed Annually
101	24	Miscellaneous	Scope of work	Training requirements per role beyond 14 CISO staff? Are lab/training environments available?	Please refer to the RFP for guidance. The bidder is required to provision and account for the lab environment and training environment as part of the proposal.
102	37	12.14 - Liquidated Damages	Liquidated Damages	Please cap the overall LD as 10% as on page 37 it is mentioned as 10% and on page 38 it is mentioned as 25%. Can this be amended as - In no event shall the over all LD levied under this RFP/ contract ever exceed 10 % of the total project cost	Please refer addendum for revised clause
103	38	12.16 - Limitation of Liability	Limitation of Liability	Please allow addition of below in this clause : Under no circumstance will bidders aggregate liability for all Losses ever exceed the fees received by bidder in preceding 12 months for the Service(s)/work order/purchase order to which the Losses relate.	Please be guided by the RFP
104	17 & 38	5.22 & 12.15	Idemnity & Intellectual Property Indemnity	Can this be restricted to IPR breach and bodily injury and damage to real and tangible property.	Please be guided by the RFP
105	40	12.18 - Order Cancellation	Order Cancellation	Can this clause be added from bidder side related to termination - Bidder may terminate the contract by a written notice to the Client if Bidder determine that a law, regulation, or anything having a similar import, or a circumstance (including cases where Client's ownership or constitution has changed), makes Bidder performance of the contract impermissible or in conflict with independence or professional rules applicable to Bidder.	Please be guided by the RFP
106	18	6.1	A holistic evaluation of the bank's technology environment to identify weaknesses, threats, and vulnerabilities (internal & external).	Request you to confirm if Risk Assessment has to be qualitative or quantitative	The Risk Assessment shall be hybrid in approach, incorporating both qualitative and quantitative methodologies.
107	18	6.1	A holistic evaluation of the bank's technology environment to identify weaknesses, threats, and vulnerabilities (internal & external).	Request you to confirm if re-validation is in-scope	Yes
108	18	6.3	Review of security configurations of servers, databases, network devices, cloud resources, and security appliances against industry best practices (CIS Benchmarks, NIST, RBI, ISO 27001).	Request you to confirm if the tools for conducting configuration review are to be provided by Service Provider or Bank shall provision the same	Bidder to factor the requiste tools and services to meet the requirement mentioned in the RFP
109	18	6.3	Configuration review of SIEM, SOAR, UEBA, firewalls, other security devices and network devices including rule-base evaluation, access control lists (ACLs), NAT policies, VPN settings, and logging.	Request you to confirm if the expectation is to conduct effectiveness review of security solution	Yes, the expectation includes conducting an effectiveness review of the deployed security solutions in addition to configuration assessment. The review should evaluate rule optimization, control adequacy, coverage, alert quality, and alignment with security policies and industry best practices.
110	20	6.5	Providing Information/Cyber Security Awareness material, mandatory RBI certifications and awareness sessions for board members, staff, vendors, customers & subsidiaries of the bank 3. Preparation of Information/ Cyber Security Awareness Videos, Audios, Radio Jingles, Quizzes for E-learning, Manual Booklet/Brochures, etc. for spreading Information/ Cyber Security Awareness for employees, customers and vendors of the bank.	Request you to confirm if count of videos,audios, radio jingles quizzes etc in-scope	Please be guided by RFP
111	20	6.5	Developing and producing diverse awareness materials, including videos, audio clips, radio jingles, interactive quizzes for e-learning, manual booklets, brochures, flyers, screensavers, and presentations to effectively disseminate cybersecurity best practices to employees, customers, and vendors.	Request you to confirm if count of videos,audios, radio jingles quizzes etc in-scope	Please be guided by RFP

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
112	20	6.5	6. Delivering specialized, role-based Information Security documentation and material focusing on current cyber threats, compliance standards, incident response, and secure practices relevant to different stakeholder groups. 7. Design and execution of IVR-based cyber security awareness messages for employees and stakeholders, including scripting, voice recording, and scheduled call campaigns. Messages shall focus on current cyber threats, safe digital practices, and regulatory advisories, with periodic updates aligned to emerging risks.	Request you to confirm on the count of training sessions	There is overall 3 sessions in a year Online awareness sessions, reading material, and quiz programs for Bank employees and vendor resources - Half Yearly Awareness session for Board of Directors (7–10 members) - Yearly
113	20	6.5	NA	Request you to confirm if the training sessions shall be onsite on remote	**Online Session will be conducted**
114	21	6.7.2	Conduct rule-based review of firewall and IPS policies against global standards (CIS, NIST)	Request you to confirm the no of firewalls in scope	Details shall be shared with the successful bidder
115	21	6.7.2	Conduct rule-based review of firewall and IPS policies against global standards (CIS, NIST)	Request you to confirm if Bank has deployed a firewall analyser or this will be a manual review	Yes Bank has deployed firewall analyser.
116	22	6.7.4	Review application and database architecture for security and regulatory compliance	Request you to confirm on the count of applications and databse in-scope	Critical application 37 and Non Cirtical application 20. Count fo database will be sahred with successful bider
117	22	6.7.5	Check configurations against industry benchmarks (CIS, NIST, ISO 27017/27018) and RBI guidelines.	Request you to confirm the vendor service providers in-scope	The bank is currently in the process of deploying a private cloud environment, while adoption of public cloud services is planned for a future phase.
118	23	6.7.9	Conduct Grey Teaming exercises combining offensive and defensive	Request you to confirm the count of Grey Teaming exercise	to be covered as a part of TTE
119	25	8.1	The Bidder must have experience and expertise in completing at least 1 assignment in listed each of the below service categories for a Scheduled Commercial Bank in India with minimum 1000 branches and value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP List of Service Categories: 1. Cyber Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cyber drill 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC Note: The experience for these service categories may be demonstrated through assignments carried out for one or more different clients; however, at least one completed assignment is required for each category	Request you to kindly consider BFSI entities for this clause	Please refer addendum for revised clause
120	28	8.2	The Bidder must have experience and expertise in completing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India having not less than 1000 branches during the last 3 years, as on the date of publication of the RFP	Request you to kindly consider BFSI for all the clauses in technical evaluation criteria instead of Scheduled Commercial Bank	Please refer addendum for revised clause
121	28	8.2	The Bidder must have experience and expertise in completing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India of value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP Service Categories: 1. Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cybersecurity Awareness & Content Development 5. Cyber Drill Services 6. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC	Request you to confirm our understanding that the maximum marks - 36 will be consolidated for all the services. **For example** if we submit 6 Engagement letter/PO/Agreement (one for each service) and total value is beyond 40L , then 36 marks will be awarded	Please refer addendum for the revised clause
122	34	11	B) Level 2 (L2) a. Experience of above 5 years b. Educational Qualifications: B.Tech/B.E/BCA/MCA or any other relevant graduation c. At least one of the Mandatory certifications below: CISA / CISM / CISSP / OSCP/ OSCE/relevant service certification d. At least 2 BFSI experience of conducting similar services	Request you to kindly consider ISO27001 and CEH Certification as well	Please be guided by the RFP, Bidder can propose the resource with relevant certification as required for performing the services
123	34	11	C) Level 3 (L3) a. Experience of above 7 years b. Educational Qualifications: B.Tech/B.E/BCA/MCA or any other relevant graduation c. At least Two (2) of the Mandatory certifications below: CISA / CISM / CISSP /OSCP/ OSCE/relevant service certification d. At least 3 BFSI experience of conducting similar services	Request you to kindly consider ISO27001 and CEH Certification as well	Please be guided by the RFP, Bidder can propose the resource with relevant certification as required for performing the services

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
124	38	12.16	The limitations set forth herein shall not apply with respect to: a. claims that are the subject of indemnification pursuant to infringement of third-party Intellectual Property Right, b. damage(s) occasioned by the Gross Negligence or Willful Misconduct of Service Provider, c. damage(s) occasioned by Service Provider for breach of Confidentiality Obligations, d. Regulatory or statutory fines imposed by a government or Regulatory agency for noncompliance of statutory or regulatory guidelines applicable to the Bank, provided such guidelines were brought to the notice of Service Provider. e. When a dispute is settled by the Court of Law in India. f. Loss occasioned by Non-compliance of Statutory or Regulatory Guidelines.	Request you to kindly exclude the below clause considering this exercise shall be point in time.	Please be guided by the RFP
125	NA	NA	NA	Request you to kindly consider the following clause in the scope of work section: "The provisions of this Section apply to Testing Services. Testing Services include scanning, penetration, intrusion testing or related analysis of the Client's information systems or enterprise whether by using intrusive or passive techniques and software tools. The Client hereby consents to Bidder performing the Testing Services and shall obtain all necessary consents of third party service providers of the Client to such Testing Services. If the Testing Services will be performed with respect to any information systems, applications or components that are hosted by any third party such as an internet service provider or application service provider then the consent shall be in the form separately provided by Bidder to the Client at the latter's request. The Client understands that Testing Services may result in disruptions of and/or damage to the Client's or third party's information systems and the information and data contained therein, including but not limited to denial of access to a legitimate system user, automatic shut-down of information systems caused by intrusion detection software or hardware, or failure of the information system. The Client is solely responsible for understanding the testing steps that will be performed as part of the Testing Services and for arranging alternative means of operation should such disruptions or failures occur and for all damage caused by the Testing Services. Bidder shall have no responsibility or liability for, and the Client and its affiliates shall have no recourse, and shall bring no claim, against Bidder or any Bidder Entity, or against any subcontractors, members	Please be guided by the RFP
126	NA	NA	NA	Request you to kindly consider the following clause in the scope of work section: "Bidder may terminate this Agreement, or any particular Services, immediately upon written notice to Client if Bidder reasonably determines that it can no longer provide the Services in accordance with applicable law or professional obligations. ."	Please be guided by the RFP
127	12	5.1	All MSEs having registration as per provisions of the Public Procurement Policy for Micro and Small Enterprises i.e. District Industries Centre (DIC) or Khadi and Village Industries Commission (KVIC) or Khadi and Industries Board (KVIB) or Coir Board or National Small Industries Commission (NSIC) or directorate of Handicrafts and Handlooms or Udyog Aadhaar Memorandum or any other body specified by Ministry of MSME and Start-ups (recognized by DIPP) are exempted from submission of Tender Fee and EMD only. Relevant certificates should be submitted by the bidder in this regard to avail of exemption. Bid Security Declaration should be submitted by eligible MSEs/Startups on Company's letter head with company seal and signature of the authorized person as per Annexure 3.	Request you to amend the clause to include **Medium Enterprises** registered under the Ministry of MSME for exemption from submission of Tender Fee and EMD.	Please be guided by the RFP
128	25	8.1	The bidder should be currently empaneled by CERT-In as Information Security Auditing Organizations.	Request you to change the clause to clause as: "The bidder should be empaneled by CERT-In for a **period of at least 5 years**."	Please be guided by the RFP
129	25	8.1	The Bidder should have at least 50 certified resources on its payroll, such as CEH, OSCP, CISA, CISSP, CompTIA Security+, CHFI, ISO/IEC 27001 LA/LI, eJPT or equivalent certifications	Request you to kindly revise the requirement to **20 certified resources on payroll** holding certifications such as CEH, OSCP, CISA, CISSP, CompTIA Security+, CHFI, ISO/IEC 27001 LA/LI, eJPT, or equivalent.	Please refer addedum for revised clause.
130	26	8.1	The Bidder must have experience and expertise in completing at least 1 assignment in cyber/digital forensic investigation for a BFSI in India with minimum 1000 branches during the last 3 years, as of the date of publication of the RFP Service Categories: 1. Cyber/Digital Forensic Investigation	We request you to include the experience from BFSI/Government/ Large enterprises and remove the requirement of "minimum 1000 branches", and extend the experience period from "last 3 years" to "last 5 years."	Please refer addendum for the revised clause

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
131	28	8.2	The bidder should have a minimum turnover per annum in India for each of the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth 1. Point 1: >40 Crores and <=60 Crore 2. Point 1: >60 Crores and <=80 Crore 3. Point 1: >80 Crores	Request you to amend the clause to consider average annual turnover for the past 3 financial years, instead of minimum turnover in each individual year.	Please refer addendum for revised clause
132	25	8.1	The Bidder must have experience and expertise in completing at least 1 assignment in listed each of the below service categories for a Scheduled Commercial Bank in India with minimum 1000 branches and value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP List of Service Categories: 1. Cyber Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cyber drill 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC	We would like you to kindly consider including experience with BFSI institutions, Commercial Banks, and Private Organizations, and to consider removal of the "minimum 1000 branches" requirement from the clause.	Please refer addendum for revised clause
133	29	8.2	The Bidder must have experience and expertise in completing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India of value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP Number of assignments per service: 1. 2 assignments → 3 Marks 2. 3 assignments → 4 Marks 3. 4 assignments → 5 marks 4. 5 assignments → 6 marks	We request you to kindly consider including experience with BFSI institutions, Commercial Banks, and Private Organizations, in addition to Scheduled Commercial Banks. We also request removal of the minimum order value requirement from the specified activities. Further, we seek clarification on the technical evaluation criteria—specifically whether submission of one qualifying work order per service category would be sufficient for eligibility and scoring. In case multiple completed assignments are required for higher technical marks, we request consideration to extend the experience period from 3 years to 5 years.	Please refer addendum for revised clause
134	12	EMD	EMD Amount- 5100000	We request clarification on whether the EMD may be submitted through Demand Draft (DD) or NEFT/RTGS, in addition to the modes specified in the bid document. Further, we also request clarification on the acceptable modes of submission for the Performance Bank Guarantee (PBG).	Please be guied by the RFP, refer section 5.10: Earnest Money Deposit (EMD)
135	26	**8 - 8.1 (7)**	The Bidder must have experience and expertise in completing at least 1 assignment in cyber/digital forensic investigation for a BFSI in India with minimum 1000 branches during the last 3 years, as of the date of publication of the RFP Service Categories: 1. Cyber/Digital Forensic Investigation	**"We request to modify this clasue as** **"**The Bidder must have completed at least one cyber/digital forensic investigation assignment for a BFSI in India with a minimum of 1000 branches **or any Government organization or in any Large scale Enterprises"**	Please refer addendum for the revised clause
136	26	**8 - 8.1 (6)**	The Bidder must have experience and expertise in completing at least 1 assignment in listed each of the below service categories for a Scheduled Commercial Bank in India with minimum 1000 branches and value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP List of Service Categories: 1. Cyber Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cyber drill 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC Note: The experience for these service categories may be demonstrated through assignments carried out for one or more different clients; however, at least one completed assignment is required for each category	We Request to modify this clause as "The Bidder must have experience and expertise in completing at least 1 assignment in listed each of the below service categories for a Scheduled Commercial Bank in India with minimum 1000 branches **/ Any Govrnment Organization / any large scale enterprises and Cumulative** value not less than ~~**INR 40**~~ **20 Lakhs** during the last ~~**3**~~ **7** years, as on the date of publication of the RFP List of Service Categories: 1. Cyber Risk Assessment / **IR Comporomise assessment support** 2. Configuration and code Review / VAPT 3. Ransomware Readiness Services/Drill / **/ Ransomewaren incident handling support** 4. Cyber drill / **Table top simulation / TTX** 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC Note: The experience for these service categories may be demonstrated through assignments carried out for one or more different clients; however, at least one completed assignment is required for each category"	Please refer addendum for revised clause
137	27	**8 - 8.1 (13)**	To avoid conflict of interest the successful bidder or its subsidiary or its associate or sister company or its holding company should not be the NextGEN SOC /IT Security /SOC vendor/Consultant of the bank under the existing or new contract	As this is restricted clause request you to remove this clause ensuring broader participation, competitive pricing, and access to best-in-class expertise,	Please refer addendum for revised clause

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
138	Page - 18	6.1		**6.1.1** Please provide the total count along with environment-wise split (Production / UAT / DR, if applicable): Systems (Servers/Endpoints/VMs): Databases (along with type – e.g., Oracle, SQL, etc.): Applications (Internal / Internet-facing): Business / IT Processes covered under scope:6.1.9 Description of Third Party Services used by PSB - **6.1.9** Kindly provide a description of third-party services currently utilized by the Bank, including but not limited to: Cloud service providers Managed security services Payment gateways Core banking vendors Any outsourced IT or SOC services **6.1.9** Please share complete location details including city and setup type for: Primary Data Centre (DC): Disaster Recovery (DR) Site: Near DR (NDR) / Alternate Processing Centres:	DC- Navi Mumbai - Qty 1 DR- Noida - Qty 1 NDR- Navi Mumbai - Qty 1
139	18	6.3		**6.3.1** Please provide the total count along with environment-wise breakup (Production / UAT / DR / NDR, if applicable): Servers (Physical / Virtual) Databases (with DB type – Oracle / MS SQL / MySQL / PostgreSQL / etc.) Network Devices (Routers, Switches, Load Balancers, Wireless Controllers, etc.) Cloud Resources (AWS / Azure / GCP – instances, storage, containers, serverless components, etc.) Security Appliances (Firewall, WAF, IPS/IDS, Proxy, EDR, SIEM, DLP, etc. – along with OEM details) **6.3.2** Kindly provide the total number of devices under each platform: Windows (Server/Desktop versions – specify versions if possible) Linux (RHEL, CentOS, Ubuntu, SUSE, etc.) Other Platforms (Unix, AIX, Solaris, Containers, Kubernetes, etc.) **6.3.6** Please provide: Total number of Application Servers Technology stack (e.g., Java, .NET, WebLogic, WebSphere, Tomcat, IIS, etc.) Internet-facing vs Internal application servers HA / Cluster configuration details (if applicable)	Details shall be shared with the successful bidder
140	19	6.4		Request you to please share the previous cyber attack history report, if available. This information will help us understand the historical threat landscape, assess existing control gaps, and align the proposed solution more effectively. If required, you may share a sanitized version of the report for confidentiality purposes.	Details shall be shared with the successful bidder
141	20	6.6		Request you to kindly help with the **Frequency of message updates**	Please be guided by RFP
142	20	6.6		Request you to kindly help with the **Drill Frequency during year**	Please refer BOM/Annexure 15
143	12	5.10 (1)	The bidder shall furnish Noninterest earning Earnest Money Deposit (EMD) amount as mentioned in the Bid Schedule by way of Bank Guarantee drawn on any Scheduled Bank in India (except Cooperative Bank, RRB & Punjab & Sind Bank) in favor of Punjab & Sind Bank, payable at Delhi.	Suggest to consider **Insurance Surety Bond** in lieu of BG. Suggest to consider Insurance Bond in lieu of BG. As this is is permitted and widely accepted across Government and PSU procurements.	Please be guided by the RFP
144	13	5.11	Security Deposit / Performance Guarantee should be submitted by way of Bank Guarantee in favor of Punjab & Sind Bank payable at Delhi / Bank Guarantee may be obtained from any of the Scheduled Commercial Banks (except Cooperative Bank, RRB & Punjab & Sind Bank)	Suggest to consider **Insurance Surety Bond** in lieu of BG. As this is is permitted and widely accepted across Government and PSU procurements.	Please be guided by the RFP

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
145	25	8 EVALUATION CRITERIA	The Bidder must have experience and expertise in completing at least 1 assignment in listed each of the below service categories for a Scheduled Commercial Bank in India with minimum 1000 branches and value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP List of Service Categories: 1. Cyber Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cyber drill 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC Note: The experience for these service categories may be demonstrated through assignments carried out for one or more different clients; however, at least one completed assignment is required for each category	Request to modify the clause as below: The Bidder must have experience and expertise ~~in completing~~ of at least 1 assignment in listed each of the below service categories for a ~~Scheduled Commercial Bank~~ BFSI in India with minimum 1000 branches/ office locations/ Regulatory bodies and value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP List of Service Categories: 1. Cyber Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cyber drill 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC Note: The experience for these service categories may be demonstrated through assignments carried out for one or more different clients; however, at least one ~~completed~~ assignment is required for each category	Please refer addendum for revised clause
146	25	8 EVALUATION CRITERIA	1. PO/Contract Copy 2. Client Credential/client Confirmation Documentary evidence should clearly showcase the service provided	Request to modify the clause as below: 1. PO/Contract Copy; 2. Client Credential/client Confirmation or invoice copy with payment proofs/ CA certificate Documentary evidence should clearly showcase the service provided	Please refer addendum for revised clause
147	26	8 EVALUATION CRITERIA	The Bidder must have experience and expertise in completing at least 1 assignment in cyber/digital forensic investigation for a BFSI in India with minimum 1000 branches during the last 3 years, as of the date of publication of the RFP Service Categories: 1. Cyber/Digital Forensic Investigation	Request to modify the clause as below: The Bidder must have experience and expertise in completing at least 1 assignment in cyber/digital forensic investigation for a BFSI in India ~~with minimum 1000 branches~~ during the last 3 years, as of the date of publication of the RFP Service Categories: 1. Cyber/Digital Forensic Investigation	Please refer addendum for the revised clause
148	26	8 EVALUATION CRITERIA	1. PO/Contract Copy 2. Client Credential/client Confirmation Documentary evidence should clearly showcase the service provided	Request to modify the clause as below: 1. PO/Contract Copy; 2. Client Credential/client Confirmation or invoice copy with payment proofs/ CA certificate Documentary evidence should clearly showcase the service provided	Please refer addendum for revised clause
149	27	8 EVALUATION CRITERIA	To avoid conflict of interest the successful bidder or its subsidiary or its associate or sister company or its holding company should not be the NextGEN SOC /IT Security /SOC vendor/Consultant of the bank under the existing or new contract	We are empanelled with Punjab & Sind bannk as a CERT-In Certified Auditors of Bank (Ref RFP No. GEM/2024/B/5579094 dated 06-11-2024). Kindly clarify whether the conflict of interest clause is applicable or there is no binding on us for participation and is applicable only on vendors and consultants but not auditors	Please refer addendum for revised clause
150	28	8 EVALUATION CRITERIA	The Bidder must have experience and expertise in completing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India having not less than 1000 branches during the last 3 years, as on the date of publication of the RFP Service Categories: 1. Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cybersecurity Awareness & Content Development 5. Cyber Drill Services 6. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC	Request to modify the clause as below: The Bidder must have experience and expertise ~~in completing~~ of at least 1 assignment in each of the service categories listed below for a ~~Scheduled Commercial Bank~~ BFSI in India having not less than 1000 branches/ office locations/ Regulatory bodies during the last 3 years, as on the date of publication of the RFP Service Categories: 1. Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cybersecurity Awareness & Content Development 5. Cyber Drill Services 6. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC	Please refer addendum for revised clause
151	29	8 EVALUATION CRITERIA	The Bidder must have experience and expertise in completing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India of value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP Service Categories: 1. Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cybersecurity Awareness & Content Development 5. Cyber Drill Services 6. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC	Request to modify the clause as below: The Bidder must have experience and expertise ~~in completing~~ of atleast 1 assignment in each of the service categories listed below for a ~~Scheduled Commercial Bank~~ BFSI in India of value not less than INR ~~40~~ 25 Lakhs during the last 3 years, as on the date of publication of the RFP Service Categories: 1. Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cybersecurity Awareness & Content Development 5. Cyber Drill Services 6. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC	Please refer addendum for revised clause
152	30	8 EVALUATION CRITERIA	The Bidder must have experience and expertise in completing assignment in cyber/digital forensic investigation for a BFSI not less than 1000 Branches in India during the last 3 years, as of the date of publication of the RFP. Service Categories: 1. Cyber/Digital Forensic Investigations	Request to modify the clause as below: The Bidder must have experience and expertise ~~in completing assignment~~ in cyber/digital forensic investigation for a BFSI/ Regulatory bodies ~~not less than 1000 Branches~~ in India during the last 3 years, as of the date of publication of the RFP. Service Categories: 1. Cyber/Digital Forensic Investigations	Please refer addendum for revised clause

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
153		Additional Claue	Limitation of the Bidder's Liability towards the Purchaser	Tenderer (and any others for whom Services are provided) shall not recover from the Supplier, in contract or tort, under statute or otherwise, any amount with respect to loss of profit, data or goodwill, or any other consequential, incidental, indirect, punitive, or special damages in connection with claims arising out of this Agreement or otherwise relating to the Services, whether or not the likelihood of such loss or damage was contemplated. Tenderer (and any others for whom Services are provided) shall not recover from the Supplier, in contract or tort, including indemnification obligations under this contract, under statute or otherwise, aggregate damages in excess of the fees actually paid for the Services that directly caused the loss in connection with claims arising out of this Agreement or otherwise relating to the Services	Please be guided by the RFP
154		Additional Claue	Non-solicitation	Bidder shall not hire employees of Tenderer or solicit or accept solicitation (either directly, indirectly, or through a third party) from employees of Tenderer directly involved in this contract during the period of the contract and one year thereafter.	Please be guided by the RFP
155		Additional Claue	Force Majeure	1) Bidder shall not be liable for forfeiture of its performance security, Liquidated damages or termination for default, if any to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure. 2) For purposes of this Clause, "Force Majeure" means an event explicitly beyond the reasonable control of the Contractor and not involving the contractor's fault or negligence and not foreseeable. Such events may be due to or as a result of or caused by act of God, wars, insurrections, riots, earth quake and fire, revolutions, civil commotion, floods, epidemics, quarantine restrictions, trade embargos, declared general strikes in relevant industries, satellite failure, act of Govt. of India, events not foreseeable but does not include any fault or negligence or carelessness on the part of the parties, resulting in such a situation. In the event of any such intervening Force Majeure, either party shall notify the other in writing of such circumstances or the cause thereof immediately within five calendar days. 3) Unless otherwise directed by Tenderer in writing, the selected contractor shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event. 4) In such a case the time for performance shall be extended by a period(s) not less than duration of such delay. If the duration of delay continues beyond a period of three months, Tenderer and the biddershall hold consultations in an endeavour to find a solution to the problem. 5) Notwithstanding above, the decision of Tenderer shall be final and binding on the bidder regarding	Please be guided by the RFP
156		Additional Claue	Termination for Convenience	1) In case of termination, Tenderer shall pay the bidder for all work-in progress, Services already performed, and expenses incurred by the bidder upto and including the effective date of the termination of this Agreement. 2) Tenderer shall be entitled to terminate/cancel the purchase order at any time for the balance order quantity which is within the delivery schedule with no liability on either side and without assigning any reason thereof. However, the purchase order for the quantity which has already been offered for inspection shall not be cancelled and supply of the same shall be availed in due course of time. 3) Bidder may terminate/cancel the contract by giving a written notice of 30 days in case: a) Its invoices are not paid on time b) If Tenderer fails to comply with the terms of agreement	Please be guided by the RFP
157		Additional Claue	Retention of copies	On payment of all bidder fees in connection with the Contract, Tenderer shall obtain a non-exclusive license to use within its internal business, subject to the other provisions of this Contract, any Deliverables or work product for the purpose for which the Deliverables or work product were supplied. bidder retains all rights in the Deliverables and work product, and in any software, materials, know-how and/or methodologies that bidder may use or develop in connection with the Contract.	Please be guided by the RFP
158		Additional Claue	Non-Exclusivity	It is agreed that the services are being rendered on a non-exclusive basis and the bidder shall have the right to pursue business opportunities that it may in its sole discretion deem appropriate.	Please be guided by the RFP
159	25	8 EVALUATION CRITERIA 8.1 Eligibility evaluation requirements	The Bidder should have at least 50 certified resources on its payroll, such as CEH, OSCP, CISA, CISSP, CompTIA Security+, CHFI, ISO/IEC 27001 LA/LI, eJPT or equivalent certifications.	For wider participation we request tender inviting authority to please ammend this clause as: The Bidder should have at least 10 certified resources on its payroll, such as CEH, OSCP, CISA, CISSP, CompTIA Security+, CHFI, ISO/IEC 27001 LA/LI, eJPT or equivalent certifications.	Please refer addedum for revised clause.

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
160	25	8 EVALUATION CRITERIA 8.1 Eligibility evaluation requirements	The Bidder must have experience and expertise in completing at least 1 assignment in listed each of the below service categories for a Scheduled Commercial Bank in India with minimum 1000 branches and value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP List of Service Categories: 1. Cyber Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cyber drill 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC Note: The experience for these service categories may be demonstrated through assignments carried out for one or more different clients; however, at least one completed assignment is required for each category	For wider participation we request tender inviting authority to please ammend this clause as: The Bidder must have experience and expertise in completing at least any 3 assignment out of 7 service categories for a Scheduled Commercial Bank/PSU/Central Government/State Government/Private Organization in India and value not less than INR 20 Lakhs during the last 5 years, as on the date of publication of the RFP List of Service Categories: 1. Cyber Risk Assessment OR ISO27001 2. Configuration and code Review OR Devsecops (AppSec & GRC implementation) 3. Ransomware Readiness Services/Drill/DPDP Assessment/Incident Response Services/or CCMP 4. Cyber drill /ISMS Implementation 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC 6. Fraud Risk Management 7.Cybersecurity Awareness Content Development Note: The experience for these service categories may be demonstrated through assignments carried out for one or more different clients. **Documentary Proof:** **Work Order or Client Credential or email confirmation from client**	Please refer addendum for revised clause
161	28	8.2 Technical evaluation requirements	The Bidder must have experience and expertise in completing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India having not less than 1000 branches during the last 3 years, as on the date of publication of the RFP Service Categories: 1. Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cybersecurity Awareness & Content Development 5. Cyber Drill Services 6. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC Number of assignments per service: 1. 2 assignments → 3 Marks 2. 3 assignments → 4 Marks 3. 4 assignments → 5 marks 4. 5 assignments → 6 marks Maximum marks – 36 marks Scoring will be conducted for each service individually and then consolidated to determine the highest overall score	For wider participation we request tender inviting authority to please ammend this clause as: The Bidder must have experience and expertise in completing at least 3 assignment out of 7 service categories assignment in listed below for a Scheduled Commercial Bank having not less than 1000 branches/PSU/Central Government/State Government/Private Organization in India during the last 5 years, as on the date of publication of the RFP List of Service Categories: 1. Cyber Risk Assessment OR ISO27001 2. Configuration and code Review OR Devesecops (AppSec & GRC implementation) 3. Ransomware Readiness Services/Drill/DPDP Assessment/Incident Response Services/or CCMP 4. Cyber drill /ISMS Implementation 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC 6. Fraud Risk Management 7.Cybersecurity Awareness Content Development Documentary Proof: Work Order or Client Credential or email confirmation from client	Please refer addendum for revised clause
162	29	8.2 Technical evaluation requirements	The Bidder must have experience and expertise in completing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India of value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP Service Categories: 1. Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cybersecurity Awareness & Content Development 5. Cyber Drill Services 6. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC Number of assignments per service: 1. 2 assignments → 3 Marks 2. 3 assignments → 4 Marks 3. 4 assignments → 5 marks 4. 5 assignments → 6 marks Maximum marks – 36 marks Scoring will be conducted for each service individually and then consolidated to determine the highest overall score.	For wider participation we request tender inviting authority to please ammend this clause as: The Bidder must have experience and expertise in completing at least 3 assignment out of 7 service categories assignment in listed below for a Scheduled Commercial Bank having not less than 1000 branches/PSU/Central Government/State Government/Private Organization in India of value not less than INR 20 Lakhs during the last 5 years, as on the date of publication of the RFP. List of Service Categories: 1. Cyber Risk Assessment OR ISO27001 2. Configuration and code Review OR Devesecops (AppSec & GRC implementation) 3. Ransomware Readiness Services/Drill/DPDP Assessment/Incident Response Services/or CCMP 4. Cyber drill /ISMS Implementation 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC 6. Fraud Risk Management 7.Cybersecurity Awareness Content Development Documentary Proof: Work Order or Client Credential or email confirmation from client	Please refer addendum for revised clause
163	29	8.2 Technical evaluation requirements	The Bidder must have experience and expertise in completing assignment in cyber/digital forensic investigation for a BFSI not less than 1000 Branches in India during the last 3 years, as of the date of publication of the RFP. Service Categories: 1. Cyber/Digital Forensic Investigations BFSI service marks depend on number of assignments per service: 1. 2 assignments → 7 Marks 2. 3 assignments → 10 Marks 3. 4 assignments → 14 Marks 4. 5 assignments → 18 marks Maximum marks – 18 marks	For wider participation we request tender inviting authority to please ammend this clause as: The Bidder must have experience and expertise in completing assignment in cyber/digital forensic/Cyber Security Sevices for a BFSI not less than 1000 Branches/PSU/Central Government/State Government/Private Organization in India during the last 5 years, as of the date of publication of the RFP. Service Categories: 1. cyber/digital forensic/Cyber Security Services Documentary Proof: Work Order or Client Credential or email confirmation from client	Please refer addendum for revised clause

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
164	28	8 EVALUATION CRITERIA	"The Bidder must have experience and expertise in completing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India having not less than **1000 branches** during the last 3 years, as on the date of publication of the RFP"	We request the bank to please allow Scheduled Commercial Bank in India having not less than **700 branches**.	Please refer addendum for revised clause
165	35	12 TERMS AND CONDITIONS	"The selected bidder shall not subcontract or permit anyone to perform any of the work, service or other performance required under the contract."	Kindly request the bank to please **allow subcontracting** under the contract.	Please be guided by the RFP
166	34	11 SKILL SET AND EXPERIENCE REQUIREMENTS OF RESOURCES:	For any of the services bidder A) Level 1 (L1) a. Experience of above 2 years b. Educational Qualifications: B.Tech/B.E/BCA/MCA or any other relevant graduation c. Minimum one of below Mandatory Certifications: CEH/LPT/CCNA/ ISO 27001 LA/LI/ITIL/relevant service certification or Certifications as per Level 2 or Level 3 d. At least 1 BFSI experience of conducting similar services B) Level 2 (L2) a. Experience of above 5 years b. Educational Qualifications: B.Tech/B.E/BCA/MCA or any other relevant graduation c. At least one of the Mandatory certifications below: CISA / CISM / CISSP / OSCP / OSCE/relevant service certification d. At least 2 BFSI experience of conducting similar services C) Level 3 (L3) a. Experience of above 7 years b. Educational Qualifications: B.Tech/B.E/BCA/MCA or any other relevant graduation c. At least Two (2) of the Mandatory certifications below: CISA / CISM / CISSP / OSCP/ OSCE/relevant service certification d. At least 3 BFSI experience of conducting similar services	Kindly provide the details of the count required for L1, L2 & L3.	Bidder is required to right size and meet the scope mentioned in the RFP
167	25	8 EVALUATION CRITERIA	6. The Bidder must have experience and expertise in completing at least 1 assignment in listed each of the below service categories for a Scheduled Commercial Bank in India with **minimum 1000 branches** and value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP	We request the bank to please allow Scheduled Commercial Bank in India having not less than **700 branches.**	Please refer addendum for revised clause
168	26	8 EVALUATION CRITERIA	The Bidder must have experience and expertise in completing at least 1 assignment in cyber/digital forensic investigation for a BFSI in India with minimum 1000 branches during the last 3 years, as of the date of publication of the RFP Service Categories: 1. Cyber/Digital Forensic Investigation	We request the bank to please allow Scheduled Commercial Bank in India having not less than **700 branches**	Please refer addendum for the revised clause
169	25	Eligibility criteria	The Bidder must have experience and expertise in completing at least 1 assignment in listed each of the below service categories for a Scheduled Commercial Bank in India with minimum1000 branches and value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP List of Service Categories: 1. Cyber Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cyber drill 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC Note: The experience for these service categories may be demonstrated through assignments carried out for one or more different clients; however, at least one completed assignment is required for each categor	We Request the Bank to Amend the clause to - The **Bidder/OEM** must have experience and expertise in completing at least 1 assignment in listed each of the below service categories for a Scheduled Commercial Bank in India with minimum1000 branches and value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP List of Service Categories: 1. Cyber Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cyber drill 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC Note: The experience for these service categories may be demonstrated through assignments carried out for one or more different clients; however, at least one completed assignment is required for each categor	Please refer addendum for revised clause
170	26	Eligibility criteria	The Bidder must have experience and expertise in completing at least 1 assignment in cyber/digital forensic investigation for a BFSI in India with minimum 1000 branches during the last 3 years, as of the date of publication of the RFP Service Categories: 1. Cyber/Digital Forensic Investigation	We Request the Bank to Amend the clause to - The **Bidder/ OEM** must have experience and expertise in completing at least 1 assignment in cyber/digital forensic investigation for a BFSI in India with minimum 1000 branches during the last 3 years, as of the date of publication of the RFP Service Categories: 1. Cyber/Digital Forensic Investigation	Please be guided by the RFP

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
171	26	Eligibility criteria	The Bidder should have at least 50 certified resources on its payroll, such as CEH, OSCP, CISA, CISSP, CompTIA Security+, CHFI, ISO/IEC 27001 LA/LI, eJPT or equivalent certifications	We Request the Bank to Amend the clause to - The Bidder should have at least **25** certified resources on its payroll, such as CEH, OSCP, CISA, CISSP, CompTIA Security+, CHFI, ISO/IEC 27001 LA/LI, eJPT or equivalent certifications	Please refer addendum for the revised clause
172	35	12 TERMS AND CONDITIONS	"The selected bidder shall not subcontract or permit anyone to perform any of the work, service or other performance required under the contract."	Is the Consortium allowed to bid in this tender	Consortium/JV/Sub-Contracting not allowed.
173	26	Eligibility criteria		Is there any relaxation for MSME bidders, in terms of Turnover and qualification criteria.	Please be guided by the RFP
174	25	8.1	The bidder should have a minimum turnover of INR 40 crore per annum in India for each of the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth.	**We kindly request you to please change the Criteria as below:** The bidder should have an average turnover of INR 20 crore in India past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth.	Please refer addendum for revised clause
175	28	1	The bidder should have a minimum turnover per annum in India for each of the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth 1. Point 1: >40 Crores and <=60 Crore 2. Point 1: >60 Crores and <=80 Crore 3. Point 1: >80 Crores	The bidder should have a minimum turnover per annum in India for each of the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth 1. Point 1: >5 Crores and <=10 Crore 2. Point 1: >10 Crores and <=15 Crore 3. Point 1: >15 Crores	Please refer addendum for revised clause
176	25	Eligibility criteria	The Bidder must have experience and expertise in completing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India having not less than 1000 branches during the last 3 years, as on the date of publication of the RFP Service Categories: 1. Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cybersecurity Awareness & Content Development 5. Cyber Drill Services 6. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC	The Bidder must have experience and expertise in completing at least 3 assignment in out of the categories listed below for a Scheduled Commercial Bank in India having not less than 1000 branches during the last 3 years, as on the date of publication of the RFP Service Categories: 1. Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cybersecurity Awareness & Content Development 5. Cyber Drill Services 6. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC	Please refer addendum for revised clause
177	29	3	The Bidder must have experience and expertise in completing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India of value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP. Service Categories: 1. Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cybersecurity Awareness & Content Development 5. Cyber Drill Services 6. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC	The Bidder must have experience and expertise in completing at least 3 assignment in out of the categories listed below for a Scheduled Commercial Bank in India of value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP Service Categories: 1. Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cybersecurity Awareness & Content Development 5. Cyber Drill Services 6. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC	Please refer addendum for revised clause
178	30	4	The Bidder must have experience and expertise in completing assignment in cyber/digital forensic investigation for a BFSI not less than 1000 Branches in India during the last 3 years, as of the date of publication of the RFP. 1. Cyber/Digital Forensic Investigations 1. 2 assignments → 7 Marks 2. 3 assignments → 10 Marks 3. 4 assignments → 14 Marks 4. 5 assignments → 18 marks	The Bidder must have experience and expertise in completing assignment in cyber/digital forensic investigation for a BFSI not less than 1000 Branches in India during the last 3 years, as of the date of publication of the RFP. 1. Cyber/Digital Forensic Investigations 1. 1 assignments → 7 Marks 2. 2 assignments → 10 Marks 3. 3 assignments → 14 Marks 4. 4 assignments → 18 marks	Please refer addendum for revised clause
179	5	1	Last Date and Time for submission of Bids : 13/03/2026 at 3:00 PM	We request Punjab Sindh Bank to extend the bid submission date for 2 weeks till 27th March 2026.	Refer Addendum for the revised clause
180	18	6.1	Physical Security Risk assessment of Data Centre , Data Recovery and NDR centres.	Kindly confirm the locations of Data Centre, DR, and NDR sites requiring assessment.	DC- Navi Mumbai - Qty 1 DR- Noida - Qty 1 NDR- Navi Mumbai - Qty 1
181	18	6.2	Forensic Investigation	1. How many incidents (approx.) are expected annually for forensic investigation? 2. What device types are typically in scope: servers, endpoints, mobile, cloud, ATM switch, CBS, etc.? 3. Are cloud workloads (AWS, Azure, GCP) included in the forensic scope? 4. Are third-party-managed assets included in incident investigations? 5. Please confirm whether the forensic work/investigation is required to be performed completely on-premises, or if we are permitted to use our secure, in-house lab to support quicker analysis. 6. Do we need to include all associated hardware costs (such as hard drives, license fees, etc.) in the proposal, or will these be provided by the bank.	1. Details will be shared with successfull bidder. Bidder to provide the rate as per the BOM 2. Details will be shared with successfull bidder 3. Yes 4. Yes 5. The engagement will be conducted entirely within the bank's on-premises environment. Remote access via VPN will not be available, and there is no separate lab infrastructure for testing. Bidders are requested to consider these constraints and plan their approach accordingly to ensure smooth and effective service delivery. 6. Yes

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
182	18	6.2	7. Create and maintain an electronic audit trail or manual record of all processes, including work-papers, applied to gather and examine relevant evidence in such a way to ensure even third parties should be able to examine those processes and achieve the same result.	Please clarify. Does an approach and methodology section in the incident report meet the expectation? Please clarify if KPMG can also retain a copy of the working papers for internal risk processes.	1. The Bank expects an electronic or manual audit trail that fully documents the processes, work-papers, and evidence used, in a manner that allows third parties to independently review and reproduce the results. 2. The documents are solely for bank use and can not be shared by any third party or bidder
183	18	6.3	Review of security configurations of servers, databases, network devices, cloud resources, and security appliances against industry best practices	We request Punjab Sindh Bank to provide the count of servers, databases, endpoints, cloud resources, network/security devices, and application servers to be reviewed.	Details shall be shared with the successful bidder
184	18	6.1	Mapping to RBI cybersecurity framework and ISO 27001	Is Bank has the ISO 27001 certification What is the date of Certification	Yes, bank has ISO/IEC 27001 certification. If required, documents will be shared with successful bidder
185	18	6.1	Physical Security Risk assessment of Data Centre , Data Recovery and NDR centres.	Can you please share the locations of Data Centre , Data Recovery and NDR centres.	DC- Navi Mumbai - Qty 1 DR- Noida - Qty 1 NDR- Navi Mumbai - Qty 1
186	18	6.1	To assess adequacy of privacy and data protection controls	Is Digital Personal Data Protection (DPDP) part of the activity ?	Yes, the Risk Assessment service explicitly includes evaluation of compliance with applicable privacy and data protection frameworks.
187	19	6.3	* Configuration review of SIEM, SOAR, UEBA, firewalls, other security devices and network devices including rule-base evaluation, access control lists (ACLs), NAT policies, VPN settings, and logging. * Examination of security logging and monitoring Configuration, including log retention, SIEM integration, and alert rules.	Please clarify whether the configuration review is limited to security hardening and rule-base evaluation or is the expectation to also perform a detection coverage assessment (e.g., MITRE ATT&CK mapping) as part of this activity. If so, please clarify the approximate number of SIEM rules to be reviewed?	The configuration review is limited to security hardening, rule-base evaluation, and compliance of SIEM, SOAR, UEBA, firewalls, and network devices. The focus is on validating configurations, access controls, and logging practices against industry standards and organizational policies.
188	19	6.4	Ransomware Readiness Services	1. What all security solutions are being used by the bank which falls under the scope of ransomware readiness, including the count of devices ? 2. Does the Bank maintain immutable or air-gapped backups? 3. How are backups tested currently (frequency, method)? 4. Does the Bank currently have a ransomware-specific incident response playbook developed and in place? 5. What zoning standards or frameworks are currently followed (e.g., RBI Cybersecurity Framework, NIST SP 800-125, Zero Trust, internal guidelines)? 6. Do we need to prepare any additional documents that the Bank currently does not have in place?	1. Bank is in the process of implemeneting multiple security solutions such as XDR, SIEM, SOAR, UEBA, IDAM, etc. 2..Yes 3. Restoration testing is performed as per bank policy. 4. No, bidder to prepare the same if required 5. All Government of India, RBI, Regulatory & statutory framework applicable to the bank shall be complied 6. Yes
189	20	6.5	6.5 Cybersecurity Awareness & Content Development	Is any Tranining platform/tool is requried as a apart of the activity?	Bidder to right size and propose the required tools/service
190	21	6.7.2	4. Identify gaps in detection and prevention coverage for modern threats	Please confirm if the expectation is a high-level assessment of detection/prevention coverage at control-placement and configuration level rather than an in-depth analysis of all detection rule sets.	The expectation is a high-level assessment of detection and prevention coverage based on the placement and configuration of security devices such as firewalls, IPS/IDS, and WAF. The focus is on identifying potential gaps in coverage and control effectiveness at the architecture and configuration level.
191	23	6.7.9	Tabletop Exercise for Incident Response Readiness	1. Kindly clarify the expected number of scenarios per half-yearly activity and duration of each scenario. 2. Kindly clarify if the we are required to roleplay as the Incident Responder/Crisis Management Team or if the bidder is only supposed to drive the simulation to elicit a response from PSB's ISO & IT teams. 3. Kindly confirm the approximate audience and the relevant teams they may belong to. 4. Are virtual labs acceptable, or should labs be conducted on-prem? 5. Does the Bank expect hands-on labs, simulations, case studies?	1) The number of scenarios and their duration will be defined by the Bank during the period; However, bidder should plan for a typical half-yearly exercise with 3-5 scenarios, each lasting approximately 2–3 hours. 2) The bidder is expected to facilitate and drive the simulation, eliciting responses from the Bank's CISO & IT teams; 3) The audience will typically include the Bank's CISO, IT, security, IT Teams and relevant operational teams, with an approximate size of 15–25 participants per exercise. 4) Virtual labs are acceptable; however, exercises is to be conducted on-premises if required by the Bank for realistic and sensitive scenarios. 5) The exercises may include a mix of hands-on labs, simulations, and case studies as deemed appropriate by the Bank to assess incident response readiness.
192	25	6.8	4. Training to Internal CISO team members, for Incident response and forensic Investigation, should be interactive, case studies, table top exercise which includes:- - Incident handling procedures for various cyber threats (Malware , Insider threats, APTs, ransomware etc.) - Forensic evidence collection (Volatile and non-Volatile data acquisition) - Disk imaging and log analysis for forensic investigation. - Memory forensic and malware analysis techniques. - Chain of custody documentation and legal considerations) - Threat actor tracking and IOC analysis.	1. Kindly confirm if the training workshops are expected to be part of Table-top / Cyber Drills and the frequency. 2. Please confirm if demonstration would be preferred or hands-on training would be required. If hands-on training would be required, would virtual labs meet the requirement? 3. Please clarify the departments and expected number of participants in such trainings.	1. The training workshops are standalone sessions 2. The training should be interactive, combining demonstrations and hands-on exercises where feasible. 3. Target audience includes the Bank's CISO team, IT Team, IT security, and relevant security staff. Expected number of participants per session is typically 10–20 members, but may vary based on requirements.
193	25	8.1	The Bidder must have experience and expertise in completing at least 1 assignment in cyber/digital forensic investigation for a BFSI in India with minimum 1000 branches during the last 3 years, as of the date of publication of the RFP Service Categories: 1. Cyber/Digital Forensic Investigation	Can we please increase the duration to 7 Years.	Please refer addendum for the revised clause

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
194	20,21	6.6	Cyber Drill Services	1. Are these drills expected to be conducted as live, on-premise technical exercises, or will they be limited to tabletop/scenario-based simulations? 2. Are scenarios expected to mimic actual incidents the Bank has experienced ? including the incidents at ATM, Payment gateway, DC/DR etc. 3. Are cloud workloads to be included in cyber drill scenarios? 4. Kindly clarify if there is any requirement to execute scenarios to subvert the existing security systems, such as in a red-teaming scenario. If not, the scenarios can be designed to be non-invasive and non-intrusive depending on the requirement. 5. Kindly clarify if we are expected to send/execute dummy (non-malicious) payloads/emails on the systems of PSB for the purpose of the drill. If yes, kindly confirm if access to test systems or existing infrastructure will be provided to carry out the drill scenario. 6. Please clarify whether one in-depth scenario per drill will be sufficient, or if each drill is expected to include multiple scenarios. 7. What is the tool used by SOC.	1. Drills may be scenario-based or live exercises, depending on the Bank's requirement; 2. Scenarios should simulate realistic incidents, which may include previous events at CBS, ATM, Payment Gateway, DC/DR, and other critical systems. 3. Cloud workloads may be included where relevant to the drill objectives. 4. Scenarios should be non-intrusive and safe for live operations. 5. Dummy/non-malicious payloads or emails may be used; access will be provided only on designated test systems or isolated environments, not production systems. 6. Each drill may include one or multiple scenarios as deemed necessary to meet exercise objectives. 7. SOC tools and technologies will be shared with the selected bidder during drill planning, as required for scenario alignment.
195	23, 24	6.7.10	1. Review applicable and latest regulatory requirements and guidelines as issued from time to time, including RBI guidelines, IT Act, PCI DSS, ISO 27001, and other relevant frameworks. 2. Assess the bank's policies, procedures, and internal controls for alignment with current and emerging regulatory standards. 3. Identify gaps, instances of non-compliance, and areas of potential regulatory or statutory risk based on the most recent regulatory guidance. 4. Examine audit trails, logging, and monitoring mechanisms to ensure readiness for regulatory and statutory reporting in line with updated requirements. 5. Provide support and recommendations for closure and compliance of regulatory and statutory audit observations, considering the latest applicable guidelines.	Please clarify whether the review of audit trails, logging, monitoring, and compliance controls is expected to be performed only against the latest applicable regulatory guidelines and updates as they are released	The review of audit trails, logging, monitoring, and compliance controls should be performed against the applicable regulatory guidelines and its updates, including any recent notifications, circulars, or amendments issued by RBI, IT Act, PCI DSS, ISO 27001, and other relevant frameworks.
196	25	8- 8.1	The Bidder should have at least 50 certified resources on its payroll, such as CEH, OSCP, CISA, CISSP, CompTIA Security+, CHFI, ISO/IEC 27001 LA/LI, eJPT or equivalent certifications.	The Bidder should have at least **25** certified resources on its payroll, such as CEH, OSCP, CISA, CISSP, CompTIA Security+, CHFI, ISO/IEC 27001 LA/LI, eJPT or equivalent certifications. **We request you to please amend this clause**	Please refer addedum for revised clause.
197	26	8- 8.1	The Bidder must have experience and expertise in completing at least 1 assignment in listed each of the below service categories for a Scheduled 1. Cyber Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cyber drill 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC	The Bidder must have experience and expertise in completing at least **1 assignment in listed each of the below service categories for a Scheduled Commercial Bank/Enterprise/PSUs/large Corporate** in India with minimum and value not less than INR 20 Lakhs during the last 5 years, as on the date of publication of the RFP List of Service Categories	Please refer addendum for revised clause
198	27	8- 8.1	The Bidder must have experience and expertise in completing at least 1 assignment in cyber/digital forensic investigation for a BFSI in India with minimum 1000 branches during the last 3 years, as of the date of publication of the RFP Service Categories: 1. Cyber/Digital Forensic Investigation	The Bidder must have experience and expertise in completing at least 1 assignment in cyber/digital forensic investigation for a **BFSI/Enterprise/large Corporate/PSUs** in India during the last 5 years, as of the date of publication of the RFP	Please refer addendum for the revised clause
199	1	GeM Document	Last date of submission: 13.03.2022	We request you to kindly **extend the last date of Submission by atleast 3 weeks form the date of publish of pre-bid responses** so that we can prepare a competitive bid response.	Please refer addendum for revised clause
200	25	8.1 Eligibility evaluation requirements (Point No.4)	The Bidder should have at least 50 certified resources on its payroll, such as CEH, OSCP, CISA, CISSP, CompTIA Security+, CHFI, ISO/IEC 27001 LA/LI, eJPT or equivalent certifications.	**Request to amend clause as below: The Bidder should have at least 40 certified resources on its payroll, such as CEH, OSCP, CISA, CISSP, CompTIA Security+, CHFI, ISO/IEC 27001 LA/LI, eJPT or equivalent certifications.**	Please refer addedum for revised clause.
201	26	8.1 Eligibility evaluation requirements(Point No.6)	The Bidder must have experience and expertise in completing at least 1 assignment in listed each of the below service categories for a Scheduled Commercial Bank in India with minimum 1000 branches and value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP **List of Service Categories:** 1. Cyber Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cyber drill 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC	**Request to amend clause as below:** **The Bidder must have experience and expertise in completing / phase / partial completed/Ongoing at least 1 assignment in listed each of the below service categories for a Scheduled Commercial Bank in India with minimum 1000 branches, BFSI, Government / PSU entity and value not less than INR 40 Lakhs during the last 5 years, as on the date of publication of the RFP** **List of Service Categories:** 1. Cyber Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cyber drill / Table top Exercise 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC	Please refer addendum for revised clause

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
			Note: The experience for these service categories may be demonstrated through assignments carried out for one or more different clients; however, at least one completed assignment is required for each category	Note: The experience for these service categories may be demonstrated through assignments carried out for one or more different clients; however, at least one completed assignment is required for each category	
202	26	8.1 Eligibility evaluation requirements (Point No.7)	The Bidder must have experience and expertise in completing at least 1 assignment in cyber/digital forensic investigation for a BFSI in India with minimum 1000 branches during the last 3 years, as of the date of publication of the RFP Service Categories: 1. Cyber/Digital Forensic Investigation	The Bidder must have experience and expertise in completing **/ phase / partial completed/ Ongoing** at least 1 assignment in cyber/digital forensic investigation for a BFSI in India with minimum **1000** branches, **BFSI, Government / PSU entity, private entity** during the last **5 years**, as of the date of publication of the RFP Service Categories: 1. Cyber/Digital Forensic Investigation	Please refer addendum for the revised clause
203	28	8.2 Technical evaluation requirements(Point No. 2)	The Bidder must have experience and expertise in completing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India having not less than 1000 branches during the last 3 years, as on the date of publication of the RFP	**Request to amend clause as below: The Bidder must have experience and expertise in completing/ phase/ partial completed/Ongoing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India having not less than 1000 branches, BFSI, Government / PSU entity during the last 3 years, as on the date of publication of the RFP**	Please refer addendum for revised clause
			Service Categories:	**Service Categories:**	
			1. Risk Assessment	1. Risk Assessment	
			2. Configuration and code Review	2. Configuration and code Review	
			3. Ransomware Readiness Services/Drill	3. Ransomware Readiness Services/Drill	
			4. Cybersecurity Awareness & Content Development	4. Cybersecurity Awareness & Content Development	
			5.Cyber Drill Services	5.Cyber Drill Services	
			6. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC	6. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC	
204	28	8.2 Technical evaluation requirements (Point No. 3)	The Bidder must have experience and expertise in completing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India of value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP	**Request to amend clause as below:** **The Bidder must have experience and expertise in completing, / phase/ partail completed/Ongoing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India, BFSI, Government / PSU entity of value not less than INR 40 Lakhs during the last 5 years, as on the date of publication of the RFP**	Please refer addendum for revised clause
			Service Categories:	**Service Categories:**	
			1. Risk Assessment	1. Risk Assessment	
			2. Configuration and code Review	2. Configuration and code Review	
			3. Ransomware Readiness Services/Drill	3. Ransomware Readiness Services/Drill	
			4. Cybersecurity Awareness & Content Development	4. Cybersecurity Awareness & Content Development	
			5. Cyber Drill Services	5. Cyber Drill Services /Table top Exercise	
			6. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC	6. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC	
205	29	8.2 Technical evaluation requirements (Point No. 4)	The Bidder must have experience and expertise in completing assignment in cyber/digital forensic investigation for a BFSI not less than 1000 Branches in India during the last 3 years, as of the date of publication of the RFP Service Categories: 1. Cyber/Digital Forensic Investigation	**Request to amend clause as below:** **The Bidder must have experience and expertise in completing/, / phase/ partail completed/Ongoing assignment in cyber/digital forensic investigation for a BFSI not less than 1000 Branches in India during the last 5 years, as of the date of publication of the RFP** **Service Categories:** **1. Cyber/Digital Forensic Investigation**	Please refer addendum for revised clause
206		12.14 Liquidated Damages	The overall LD during certification/sustenance will be to a maximum of 25% of the contract value.	Request to clarify LD % as in same clause it is 10% of the contract value. We would request to consider LD as 10% of the contratc vlaue	Please refer addendum for revised clause
207	-	-	Documentary proof for completed projects	We would request to consider CA certificate / Copies of Invoices for completed / phase completion proof for projects	Please refer addendum for revised clause
208		Additional Claue	Additional Clause: Limitation of the Bidder's Liability towards the Purchaser	Request you to kindly consider the clause as under: The Client (and any others for whom Services are provided) shall not recover from the Bidder, in contract or tort, under statute or otherwise, any amount with respect to loss of profit, data or goodwill, or any other consequential, incidental, indirect, punitive or special damages in connection with claims arising out of this Agreement or otherwise relating to the Services, whether or not the likelihood of such loss or damage was contemplated. The Client (and any others for whom Services are provided) shall not recover from the Bidder, in contract or tort, including indemnification obligations under this contract, under statute or otherwise, aggregate damages in excess of the fees actually paid for the Services that directly caused the loss in connection with claims arising out of this Agreement or otherwise relating to the Services	Please be guided by the RFP
209		Additional Claue	Additional Clause: Indemnity	Request you to kindly consider the clause as under: The Client shall indemnify and hold harmless the GT Entities and GT Bharat LLP for all Losses incurred in connection with any third-party Claim, except to the extent finally judicially determined to have resulted primarily from the fraud or bad faith of such GT Entity or GT Bharat LLP	Please be guided by the RFP

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
210		Additional Claue	Additional Clause: Non-solicitation	Request you to kindly consider the clause as under: During the Restricted Period, no Engagement Personnel of either party shall solicit for employment any Engagement Personnel of the other party. "Engagement Personnel" shall be defined as only those personnel of either party who a) are directly involved in the provision of Services under the applicable Statement of Work, or b) are the direct recipients of such Services. The "Restricted Period" shall be defined to include a) the Term of the applicable Statement of Work, b) a period of 12 months after the expiration of such Term, and c) for those Engagement Personnel whose involvement as a direct provider or recipient of Services ends prior to the expiration of the Term, for 12 months after such involvement ends. Provided, that this restriction shall not apply to (i) Engagement Personnel of a party who respond to general advertisements for positions with the other party, (ii) Engagement Personnel of either party who come to the other party on their own initiative without direct or indirect encouragement from the other party's Engagement Personnel, or (iii) generic recruiting activities by non-Engagement Personnel, including direct outreach by recruiters of either party who have sourced the individuals in the ordinary course of recruiting through the use of research, agencies, social media and/or other technology or tools	Please be guided by the RFP
211		Additional Claue	Additional Clause: Force Majeure	Request you to kindly consider the clause as under: Force Majeure to facilitate remote working. i. To the extent that the provision of the Services is impacted by a pandemic (including COVID19) and any reasonable concerns or measures taken to protect the health and safety interests of either Party's personnel, the Parties will work together to amend the Agreement to provide for the Services to be delivered in an appropriate manner, including any resulting modifications with respect to the timelines, location, or manner of the delivery of Services. ii. Where the Bidder Personnel are required to be present at Client's premises, the Bidder will use reasonable efforts to provide the Services on-site at Client side, provided that, in light of a pandemic the parties agree to cooperate to allow for remote working and/or an extended timeframe to the extent a. any government or similar entity implements restrictions that may interfere with provision of onsite Services; b. either party implements voluntary limitations on travel or meetings that could interfere with provision of onsite Services, or c. an bidder's resource determines that he or she is unable or unwilling to travel in light of a pandemic-related risk.	Please be guided by the RFP
212		Additional Claue	Additional Clause: Retention of Copies	Request you to kindly consider the clause as under: The Bidder shall be permitted to retain all information and documents as maybe required for legal or professional regulatory purposes, provided that such retained information remains subject to confidentiality obligations for the entire retention period.	Please be guided by the RFP
213		Additional Claue	Additional Clause: Non-Exclusivity	Request you to kindly consider the clause as under: It is agreed that the services are being rendered on a non-exclusive basis and the Bidder shall have the right to pursue business opportunities that it may in its sole discretion deem appropriate.	Please be guided by the RFP

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
214		Additional Claue	Additional Clause: Termination	Request you to kindly consider the clause as under: 1. In the event of termination of this Contract due to any cause whatsoever, the Contract with stand cancelled effective from the date of termination of this Contract 2. In case of exigency, if the Purchaser gets the work done from elsewhere, the difference in the cost of getting the work done shall be borne by the Consultant 3. Where the termination of the Contract is prior to its stipulated term on account of a Default on the part of the Consultant or due to the fact that the survival of the consultant as an independent corporate entity is threatened/ has ceased, or for any other reason, whatsoever, the Purchaser through re-determination of the consideration payable to the consultant as agreed mutually by the Purchaser and the consultant may pay the consultant for that part of the Services which have been authorized by the Purchaser and performed by the consultant up to the date of termination. Without prejudice any other rights, the Purchaser may retain such amounts from the payment due and payable by the Purchaser to the consultant as may be required to offset any losses caused to the Purchaser as a result of any act/ omissions of the consultant. In case of any loss or damage due to default on the part of the consultant in performing any of its obligations with regard to executing the Scope of Work under this Contract, the consultant shall compensate the Purchaser for any such loss, damages or other costs, incurred by the Purchaser. Additionally, other members of its team shall perform all its obligations and responsibilities under this Contract in an identical manner as were being performed before the collapse of the Bidder as described above in order to execute an effective transition and to maintain business continuity. 4.Nothing herein shall restrict the right of the Purchaser	Please be guided by the RFP
215				1. In the event of termination of this Contract due to any cause whatsoever, the Contract with stand cancelled effective from the date of termination of this Contract	
216				2. In case of exigency, if the Purchaser gets the work done from elsewhere, the difference in the cost of getting the work done shall be borne by the Consultant	
217				3. Where the termination of the Contract is prior to its stipulated term on account of a Default on the part of the Consultant or due to the fact that the survival of the consultant as an independent corporate entity is threatened/ has ceased, or for any other reason, whatsoever, the Purchaser through re-determination of the consideration payable to the consultant as agreed mutually by the Purchaser and the consultant may pay the consultant for that part of the Services which have been authorized by the Purchaser and performed by the consultant up to the date of termination. Without prejudice any other rights, the Purchaser may retain such amounts from the payment due and payable by the Purchaser to the consultant as may be required to offset any losses caused to the Purchaser as a result of any act/ omissions of the consultant. In case of any loss or damage due to default on the part of the consultant in performing any of its obligations with regard to executing the Scope of Work under this Contract, the consultant shall compensate the Purchaser for any such loss, damages or other costs, incurred by the Purchaser. Additionally, other members of its team shall perform all its obligations and responsibilities under this Contract in an identical manner as were being performed before the collapse of the Bidder as described above in order to execute an effective transition and to maintain business continuity.	
218				4.Nothing herein shall restrict the right of the Purchaser to invoke the Bank Guarantee and other Guarantees furnished hereunder, and pursue such other rights and/ or remedies that may be available to the Purchaser under law	
219				5.The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of this Contract that are expressly or by implication intended to come into or continue in force on or after such termination	

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
220	26	8.1 Eligibility evaluation requirements(Point No.6)	Point6 - the Bidder must have experience and expertise in completing at least 1 assignment in listed each of the below service categories for a Scheduled Commercial Bank in India with minimum 1000 branches and value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP. List of Service Categories: 1. Cyber Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cyber drill 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC Note: The experience for these service categories may be demonstrated through assignments carried out for one or more different clients; however, at least one completed assignment is required for each category	Restriction to Scheduled Commercial Banks (SCB) The current requirement restricting experience to Scheduled Commercial Banks limits participation significantly. Many reputed cybersecurity firms have executed large-scale and complex assignments for: • BFSI institutions (NBFCs, Insurance, Payment Banks, Fintechs) • Regulatory bodies • Government financial institutions • Large private financial institutions Cybersecurity complexity is determined by digital ecosystem, regulatory exposure, infrastructure maturity, and risk posture — not solely by SCB classification. We therefore request that experience criteria be expanded to include: BFSI organizations / Regulatory Bodies / Government Financial Institutions / Private Financial Institutions in India.	Please refer addendum for revised clause
221	26	8.1 Eligibility evaluation requirements(Point No.7)	The Bidder must have experience and expertise in completing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India having not less than 1000 branches during the last 3 years, as on the date of publication of the RFP Service Categories: 1. Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cybersecurity Awareness & Content Development 5. Cyber Drill Services 6. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC	Removal of Minimum 1000 Branch Requirement The requirement of minimum 1000 branches does not necessarily reflect the scale or complexity of cybersecurity engagements. Many digitally mature institutions operate centralized or hybrid models without extensive branch networks but manage significant transaction volumes and cyber risk exposure. We request removal of the 1000-branch condition across eligibility and technical evaluation sections.	Please refer addendum for revised clause
222	26	8.1 Eligibility evaluation requirements(Point No.6)	Point6 - the Bidder must have experience and expertise in completing at least 1 assignment in listed each of the below service categories for a Scheduled Commercial Bank in India with minimum 1000 branches and value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP. List of Service Categories: 1. Cyber Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cyber drill 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC Note: The experience for these service categories may be demonstrated through assignments carried out for one or more different clients; however, at least one completed assignment is required for each category	Removal of INR 40 Lakhs Minimum Order Value Cybersecurity engagements such as ransomware drills, forensic investigations, cyber risk assessments, and configuration reviews are often strategic in nature and may not always be high in contract value despite being enterprise-critical. We request reconsideration of the minimum INR 40 Lakhs order value requirement and suggest evaluation based on scope and impact instead of contract size.	Please refer addendum for revised clause
223	26	8.1 Eligibility evaluation requirements(Point No.7)	The Bidder must have experience and expertise in completing at least 1 assignment in cyber/digital forensic investigation for a BFSI in India with minimum 1000 branches during the last 3 years, as of the date of publication of the RFP Service Categories: 1. Cyber/Digital Forensic Investigation	Inclusion of Audit / Investigative Capabilities Alongside Forensic Investigation We request that the forensic investigation clause be expanded to include Information Security Audit / Incident Response / Cyber Investigation capabilities, as these assignments often involve investigative and forensic-level analysis even if not contractually termed as forensic engagements.	Please be guided by the RFP
224	-	-	Additional	Consideration for Presentation-Based Evaluation We further request inclusion of a structured presentation round with defined marks to assess: • Technical approach and methodology & Execution framework • Team capability & Governance and reporting model This will support qualitative assessment beyond documentary credentials. We believe the above relaxations will: • Promote fair and competitive participation • Encourage broader industry representation • Enable selection of the most technically capable partner	Please be guided by the RFP
225	12	Section 5.10	EMD	**5.10 Earnest Money Deposit: Point 5: All MSEs h**	Please be guied by the RFP, refer section 5.10: Earnest Money Deposit (EMD)

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
226	12	Section 5.10	EMD	EMD Query: EMD Amount- INR 51,00,000 Query/Clarification: We request clarification on whether the EMD may be submitted through Demand Draft (DD) or NEFT/RTGS, in addition to the modes specified in the bid document. Further, we also request clarification on the acceptable modes of submission for the Performance Bank Guarantee (PBG).	Please be guied by the RFP, refer section 5.10: Earnest Money Deposit (EMD)
227	25	Section 8.1 Eligibility	8.1 Eligibility evaluation requirements Point 3: The bidder should be currently empanelled by CERT-In as Information Security Auditing Organizations.	Query/Clarification: Request you to change the clause to clause as: The bidder should be empanelled by CERT-In for a period of at least 5 years	Please be guided by the RFP
228	25	Section 8.1 Eligibility	8.1 Eligibility evaluation requirements Point 5: The Bidder should have at least 50 certified resources on its payroll, such as CEH, OSCP, CISA, CISSP, CompTIA Security+, CHFI, ISO/IEC 27001 LA/LI, eJPT or equivalent certifications.	**Query/Clarification: Request you to kindly revise the requirement to 20 certified resources on payroll holding certifications such as CEH, OSCP, CISA, CISSP, CompTIA Security+, CHFI, ISO/IEC 27001 LA/LI, eJPT, or equivalent.**	Please refer addedum for revised clause.
229	25	Section 8.1 Eligibility	8.1 Eligibility evaluation requirements Point 6: The Bidder must have experience and expertise in completing at least 1 assignment in listed each of the below service categories for a Scheduled Commercial Bank in India with minimum 1000 branches and value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP List of Service Categories: 1. Cyber Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cyber drill 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC	Query/Clarification: We would like you to kindly consider including experience with BFSI institutions, Commercial Banks, and Private Organizations, and to consider removal of the “minimum 1000 branches” requirement from the clause.	Please refer addendum for revised clause
230	25	Section 8.1 Eligibility	8.1 Eligibility evaluation requirements Point 7: The Bidder must have experience and expertise in completing at least 1 assignment in cyber/digital forensic investigation for BFSI in India with minimum 1000 branches during the last 3 years, as of the date of publication of the RFP Service Categories: 1. Cyber/Digital Forensic Investigation	Query/Clarification: We request you to include the experience from BFSI/Government/ Large enterprises and remove the requirement of “minimum 1000 branches”, and extend the experience period from “last 3 years” to “last 5 years.”	Please refer addendum for the revised clause
231	28	Section 8.3 technical		8.2 Technical evaluation requirements Point 1: The bidder should have a minimum turnover per annum in India for each of the past 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth. 1. Point 1: >40 Crores and <=60 Crore 2. Point 1: >60 Crores and <=80 Crore 3. Point 1: >80 Crores Query/Clarification: Request you to amend the clause to consider average annual turnover for the past 3 financial years, instead of minimum turnover in each individual year.	Please refer addendum for revised clause
232	Page 28 of 73	8 EVALUATION CRITERIA	The technical bid submitted by the Bidder will be evaluated only if they fulfil the eligibility criteria as defined in section 8.1 Eligibility evaluation criteria. The technical bid evaluation will be done with a total score of 100 marks for each group. The bidders should score minimum overall 80% marks in total for further selection process. The Bidders who do not qualify the section wise cut-off or total cutoff will be dropped at this stage.	We kindly request the Bank to ammend the clause as follows: The technical bid submitted by the Bidder will be evaluated only if they fulfil the eligibility criteria as defined in section 8.1 Eligibility evaluation criteria. The technical bid evaluation will be done with a total score of 100 marks for each group. The bidders should score minimum overall 70% marks in total for further selection process. The Bidders who do not qualify the section wise cut-off or total cutoff will be dropped at this stage.	Please refer addendum for revised clause
233	Page 28 of 73	8 EVALUATION CRITERIA	S. No 2: The Bidder must have experience and expertise in completing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India having not less than 1000 branches during the last 3 years, as on the date of publication of the RFP Service Categories: 1. Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cybersecurity Awareness & Content Development 5. Cyber Drill Services 6. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC	We kindly request the Bank to ammend the clause as follows: The Bidder must have experience and expertise in completing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India having not less than 1000 branches during the last 7 years, as on the date of publication of the RFP Service Categories: 1. Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cybersecurity Awareness & Content Development	Please refer addendum for revised clause
234	Page 28 of 73	8 EVALUATION CRITERIA	Number of assignments per service: 1. 2 assignments → 3 Marks 2. 3 assignments → 4 Marks 3. 4 assignments → 5 marks 4. 5 assignments → 6 marks Maximum marks – 36 marks Scoring will be conducted for each service individually and then consolidated to determine the highest overall score	We kindly request the Bank to ammend the clause as follows: Number of assignments per service: 1. 1 assignment → 3 Marks 2. 2 assignments → 4 Marks 3. 3 assignments → 5 marks 4. 4 assignments → 6 marks Maximum marks – 36 marks Scoring will be conducted for each service individually and then consolidated to determine the highest overall score.	Please refer addendum for revised clause

Pre-Bid Query Replies
Punjab Sind Bank
GEM/2026/B/7271228

S. No	Page No.	Section	Clause/Technical Specification	Bidder's Query	Bank's Response
235	Page 29 of 73	8 EVALUATION CRITERIA	S. No 3: The Bidder must have experience and expertise in completing at least 1 assignment in each of the service categories listed below for a Scheduled Commercial Bank in India of value not less than INR 40 Lakhs during the last 3 years, as on the date of publication of the RFP Service Categories: 1. Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cybersecurity Awareness & Content Development 5. Cyber Drill Services 6. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC	May we kindly request the Bank to change the clause as follows: The Bidder must have experience and expertise in completing at least 1 assignment in listed each of the below service categories for a Scheduled Commercial Bank in India with minimum 1000 branches and value not less than INR 40 Lakhs during the last 7 years, as on the date of publication of the RFP List of Service Categories: 1. Cyber Risk Assessment 2. Configuration and code Review 3. Ransomware Readiness Services/Drill 4. Cyber drill 5. Information Security Services for review of comprehensive security Data Centre/Enterprise & Network/SOC Note: The experience for these service categories may be demonstrated through assignments carried out for one or more different clients; however, at least one completed assignment is required for each category The 40 lakhs PO value may be derived from either one or multiple PO/WO/ELs within a single financial year from a single Scheduled Commercial Bank in India having a minimum of 1,000 branches.	Please refer addendum for the revised clause
236	Page 29 of 73	8 EVALUATION CRITERIA	We kindly request the Bank to ammend the clause as follows: Number of assignments per service: 1. 2 assignments → 3 Marks 2. 3 assignments → 4 Marks 3. 4 assignments → 5 marks 4. 5 assignments → 6 marks Maximum marks – 36 marks Scoring will be conducted for each service individually and then consolidated to determine the highest overall score.	We kindly request the Bank to ammend the clause as follows: Number of assignments per service: 1. 1 assignment → 3 Marks 2. 2 assignments → 4 Marks 3. 3 assignments → 5 marks 4. 4 assignments → 6 marks Maximum marks – 36 marks Scoring will be conducted for each service individually and then consolidated to determine the highest overall score.	Please refer addendum for the revised clause
237	Page 29 of 73	8 EVALUATION CRITERIA	S. No 3: The Bidder must have experience and expertise in completing assignment in cyber/digital forensic investigation for a BFSI not less than 1000 Branches in India during the last 3 years, as of the date of publication of the RFP. Service Categories: 1. Cyber/Digital Forensic Investigations	We kindly request the Bank to ammend the clause as follows: The Bidder must have experience and expertise in completing at least 1 assignment in cyber/digital forensic investigation or digital forensic readiness assessment or malware analysis for a BFSI in India with minimum 1000 branches during the last 7 years, as of the date of publication of the RFP Service Categories: 1. Cyber/Digital Forensic Investigation	Please refer addendum for revised clause
238	Page 29 of 73	8 EVALUATION CRITERIA	BFSI service marks depend on number of assignments per service: 1. 2 assignments → 7 Marks 2. 3 assignments → 10 Marks 3. 4 assignments → 14 Marks 4. 5 assignments → 18 marks Maximum marks – 18 marks	We kindly request the Bank to ammend the clause as follows: BFSI service marks depend on number of assignments per service: 1. 1 assignment → 7 Marks 2. 2 assignments → 10 Marks 3. 3 assignments → 14 Marks 4. 4 assignments → 18 marks Maximum marks – 18 marks	Please refer addendum for revised clause