Central Bank of India

Information Security Department

Tender No. GEM/2026/B/8006355

Request for Proposal (Bid) Document

For

Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank

TABLE OF CONTENTS

1. Invitation for Tender Offers 7
2. Eligibility Criteria 12
3. EMD / Bid Security 16
4. Performance Bank Guarantee 17
5. Cost of Bidding 18
6. Detailed Scope of Work 18
7. Resource Requirement 53
8. Project Timelines 56
9. Contract Renewal 56
10. SLA compliance 56
10.1 Service Level Agreements (SLA) 56
11. Liquidated damage 57
12. Land Border Sharing Clause 57
13. Monitoring & Audit 59
14. Bid Submission 59
15. Integrity Pact 61
16. Commercial Offers 61
17. Evaluation & Acceptance 62
18. Evaluation Process 62
19. Payment Terms 70
20. Order Cancellation 73
21. Project Review 74
22. Indemnity 74
23. Confidentiality & Non-Disclosure 77
24. Force Majeure 77
25. Resolution of Disputes 78
26. Independent Contractor 79
27. Assignment 79
28. Insurance 80
29. Execution of Contract, SLA & NDA 80
30. SUCCESSFUL Bidder's Liability 80
31. Information Ownership 81

32. Inspection, Audit, Review, Monitoring & Visitations 82
33. Information Security....83
34. Intellectual Property Rights....84
35. Visitorial Rights 86
36. Termination 86
37. Exit option and Contract Re-Negotiation 88
38. Privacy & Security Safeguards....89
39. Governing Law and Jurisdiction 89
40. Compliance with Laws....90
41. Regulatory compliance 90
42. Violation of Terms 91
43. Data localization....91
44. Corrupt & Fraudulent Practices 91
45. Publicity 92
46. Applicability of preference to make in india, order 2017 (ppp-mii order) 92
48. Sustainable Sourcing....96
49. Entire Agreement; Amendments 96
50. Adherence to Cyber Security Policy....96
51. Survival and Severability....97
52. Amendments to Bidding Documents 97
53. Period of Validity....97
54. Ownership, Grant and Delivery 97
55. Last Date and Time for Submission of Bids 98
56. Authorized Signatory....98
57. Late Bids 98
58. Modifications and/or Withdrawal of Bids 98
59. Waiver....99
63. Signing of Contract....100
64. Checklist for Submission 100
65. Annexure-1 Bill of Material....102
66. Annexure 2: Conformity Letter....106
67. Annexure 3: Bidder's Information 107
68. Annexure 4: Letter for Conformity of Product as per RFP....108
69. Annexure 5: Undertaking for Acceptance of Terms of RFP....109
70. Annexure 6: Integrity Pact 110

71. Annexure 7: Non-Disclosure Agreement 115
72. Annexure 8: Performance Bank Guarantee 120
73. Annexure 9: Bid Security (Earnest Money Deposit) 123
74. Annexure 10: Bidder's Particulars 125
75. Annexure 11: NPA/PENDING LITIGATION/BLACKLISTING Undertaking 126
76. Annexure 12: Undertaking letter (Land Border Sharing) 127
77. Annexure 13: Cover Letter 130
78. Annexure 14: Pre-bid Query Format 132
79. Annexure 15: Eligibility Criteria Compliance 133
80. Annexure 16: Self declaration for compliance to RBI master direction on outsourcing of IT services 138
81. Annexure 17: GOI Guidelines for preference to Make in India 139
82. Annexure 18: Guidelines on banning of business dealing 142
83. Annexure 19: Undertaking for 2 Years Roadmap 152
84. Annexure 20: Undertaking For Information Security 153
85. Annexure 21: undertaking for authenticity of the product 154
86. Annexure 22: List of Software and Hardware Components required for implementation 155
87. Annexure 23: Proposed Team Profile 157

Definitions and Acronyms

Following terms are used in the document interchangeably to mean:

Acronym	Definition
AAA	Authentication, Authorization and Accounting framework in Networking
AD	Active Directory
AMC	Annual Maintenance Contract
API	Application Programming Interface
ASM	Attack Surface Management
ATS	Annual Technical Support
Bank/CBoI	Central Bank of India
BAS	Breach and Attack Simulation
BFSI	Banking Financial Services and Insurance
"Bidder"	Single point of contact appointed by the Bank for procurement and supply of the equipment based on the Bill of Materials shared by the Bank.
"CBS"	Core Banking Solution
"CO"	Central Office
CVC	Central Vigilance Commission
DAM	Database Activity Monitoring
DC	Data Centre of the Bank which is located at Central Office, Belapur, Mumbai
DMZ	Demilitarized Zone
DNS	Domain Name Server
DRC	Disaster Recovery Centre which is located in Hyderabad
EMD	Earnest Money Deposit
EMS	Enterprise Management System
FPS	Flows Per Second
GbE/GigE/Gbps	Gigabit Per Second
GoI	Government of India
HA	High Availability
HDD	Hard Disk Drive
HO	Head Office
INR	Indian National Rupee
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
LAN	Local Area Network
Mbps	Megabits Per Second
MPLS	Multi-Protocol Label Switching
MTBF	Mean Time before Failure
NDA	Non-Disclosure Agreement
NOC	Network Operations Centre
NMS	Network Management System
OEM	Original Equipment Manufacturer

PO	Purchase Order
RFP	Request for Proposal
RMA	Return Material Authorization
RO	Regional Office
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SCB	Scheduled Commercial Bank
SIEM	Security Information and event Management
SSD	Solid State Drive
SMTP	Simple Mail Transfer Protocol
SOAR	Security Orchestration Automation and Response
SoW	Scope of Work
SLA	Service Level Agreement
SPOC	Single Point of Contact
SSL	Secure Sockets Layer
T&C	Terms & Conditions
Tbps	Terabits per second
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TOR	Top of Rack
UAT	User Acceptance Test
VPN	Virtual Private Network
WAN	Wide Area Network
WAF	Web Application Firewall
ZO	Zonal Office
IFSCA	International Financial Services Centres Authority

1. INVITATION FOR TENDER OFFERS

Central Bank of India, The Bank, a body corporate constituted under the Banking Companies (Acquisition and Transfer of Undertaking) Act 1970 having its Central Office at Chandermukhi, Nariman Point, Mumbai-400021 hereinafter called "Bank" and having 90 Regional Offices (RO), 13 Zonal Offices (ZO) and 4600 plus branches spread across India, intends to appoint Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank. Bank invites unconditional online tender offers (Technical offer and Commercial offer) from eligible consultant for the contract period of two (2) years.

The details are given below:

Date of RFP Issue	07/09/2026
Bid Security (EMD)	An amount of Rs. 16,00,000/- (Sixteen Lacs Only) in the form of Bank Guarantee issued by a scheduled bank other than Central Bank of India for the entire period of Bid validity plus 3 months or by means of banker's cheque/ Account Payee Demand Draft /RTGS/NEFT in the account no.- 3287810289 of Central Bank of India (IFSC Code – CBIN0283154) with narration Tender ref no in favour of "Central Bank Of India" and payable at Mumbai/Navi Mumbai.
e-mail IDs for sending queries	smitcsoc@centralbank.bank.in, purcppco@centralbank.bank.in cminfosec@centralbank.bank.in
Last Date for submission of pre-bid queries	Latest by 17/09/2026 up to 16:00 hrs. As per the format given in **Annexure-14**
Date and time for Pre-Bid Meeting,	18/09/2026 at 15:00hrs.
Last Date and Time submission of Bids Mode of bid submission & online	21/10/2026 up to 15:00 hrs.
Time & Date of Opening of technical bids	22/10/2026 at 15:00 hrs.
Mode of Submission	Government e Marketplace (GeM)
Response Types	1.Technical Bid plus Bid Security/EMD 2.Commercial Bid
Address for Communication	CISO, Central Bank Of India Information Security Department, Plot no-26, Sector-11, CBD Belapur, Navi Mumbai- 400614 Mail address: smitcsoc@centralbank.bank.in, purcppco@centralbank.bank.in cminfosec@centralbank.bank.in

Contact Telephone Numbers	022- 27782529

For any clarification with respect to this RFP, the bidder may send their queries/suggestions, valuable inputs. It may be noted that all queries, clarifications, questions etc., relating to this RFP, technical or otherwise, must be in writing only and should be sent to designated email ID within stipulated time as per **Annexure 14.**

In accordance with Government of India guidelines, Micro and Small Enterprises are eligible to get tender documents free of cost and also exempted from payment of earnest money deposit upon submission of valid MSE certificate copy.

Start-ups (which are not MSEs) are exempted only from Bid security amount.

Earnest Money Deposit mentioned above must accompany all tender offers (Technical Bid) as specified in this tender document.

Tender offers will normally be opened half an hour after the closing time. Any tender received without Earnest Money Deposit (EMD) etc will be disqualified.

Technical Specifications, Terms and Conditions and various format and Performa for submitting the tender offer are described in the tender document and its Annexures.

Extant guidelines of GeM shall be applicable.

CISO,
Central Bank Of India
Information Security Department,
Plot no-26, Sector-11,
CBD Belapur, Navi Mumbai- 400614

DISCLAIMER The information contained in this Request for Proposal (RFP) document or information conveyed subsequently to bidder(s) or applicants whether verbally or in documentary form by or on behalf of Central Bank of India (Bank), is provided to the bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP is neither an agreement nor an offer and is only an invitation by Bank to the interested parties for submission of unconditional bids. The purpose of this RFP is to provide the bidder(s) with information to assist the formulation of their proposals. This RFP does not claim to contain all the information each bidder may require. Each bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP and where necessary obtain independent advice. Bank makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. Bank may in its absolute discretion, but

without being under any obligation to do so, update, amend or supplement the information in this RFP.

OBJECTIVE

In view of the rapidly evolving Cyber Security threat landscape, increasing sophistication of cyber-attacks, rise in ransomware incidents, digital frauds, supply chain threats, insider threats, and expanding attack surfaces arising from accelerated digital transformation initiatives, it has become imperative for Banks to continuously strengthen and enhance their Information Security and Cyber Security framework to ensure secure, resilient, reliable, and uninterrupted banking operations.

As part of the Nation's critical financial infrastructure, the Bank is required to maintain robust Cyber Defence capabilities to safeguard the confidentiality, integrity, availability, and resilience of its information assets, digital banking channels, applications, network infrastructure, critical systems, and customer data against emerging Cyber Threats and operational disruptions. Simultaneously, the Bank is required to align with evolving Regulatory expectations, Industry standards, Cyber resilience requirements, Governance obligations, and best practices prescribed by regulatory and statutory bodies including RBI, CERT-In, NCIIPC, IFSCA, ISO standards, and other applicable cybersecurity and technology frameworks.

The Bank recognizes that cybersecurity is not only a technology function but also a critical component of enterprise risk management, operational resilience, business continuity, governance, and strategic decision-making. Accordingly, the Bank intends to establish a comprehensive and future-ready cybersecurity governance, monitoring, assessment, assurance, and resilience framework capable of proactively identifying, preventing, detecting, responding to, and recovering from evolving cyber threats and risks.

To achieve these objectives, the Bank intends to engage an experienced, competent, and CERT-In empanelled IT & Cyber Security Advisor and Managed security service provider through this RFP for providing comprehensive Cyber Security Advisory, Assessment, Governance, Managed Security, Technical Security, Implementation Support, and Specialized Cyber Security Services for strengthening the Bank's overall cybersecurity posture, governance framework, operational resilience, security monitoring capabilities, and risk management ecosystem.

The broad objective of this RFP is to obtain specialized cybersecurity advisory services and managed security services.

The selected Bidder shall provide skilled onsite and/or on-demand resources, domain expertise, technical assessments, advisory services, implementation assistance, governance support, remediation validation, reporting, training, knowledge transfer, and other related cybersecurity

services in accordance with the scope, timelines, deliverables, service levels, and requirements defined under this RFP.

1. Brief Scope of Work

The selected Bidder shall provide comprehensive Cyber Security Advisory, Assessment, Governance, Managed Security, Technical Security, and Implementation Support Services for strengthening the Bank's existing cybersecurity framework, Cyber Security Architecture, Regulatory Compliance posture, operational resilience, security monitoring capabilities, and overall cyber defence ecosystem.

The scope of work under this RFP broadly includes the following categories:

A. Advisory Services

The Advisory Services are intended to strengthen the Bank's cybersecurity governance framework, study the security tools and technology deployed, operational resilience, risk management practices, regulatory compliance posture, and overall cybersecurity maturity across people, process, and technology domains.

Strengthen organizational cybersecurity posture and risk resilience through strategic assessment, governance, and best practices.

1. **Assessment & Roadmap**

    - Study the Security Tools and Technology deployed
    - Cyber Security Architecture / Framework
    - Evaluate current cybersecurity practices.
    - Identify gaps & risks.
    - Develop phased roadmap to strengthen security.
    - Conduct the Gap Assessment and offer suitable recommendation and suggestions for strengthening the Security posture of the Bank.

2. **Governance & Compliance**

    - Establish Policies, Standards, and Accountability.
    - Implement Risk Management and Regulatory Compliance Frameworks.
    - Develop SOPs, best practices for daily operations.
    - Develop suitable Dashboards for monitoring on continuous basis and for Executing oversight.

3. **Controls & Incident Readiness**

    - Assess and enhance Security Controls (technical, administrative, physical).
    - Strengthen Incident Response and Threat Management Capabilities.

- Advise effective log monitoring tools.

4. **Awareness & Third-Party Risk**

    - Conduct Staff Training programs.
    - Evaluate and monitor vendor/partner security posture.

5. **Monitoring & Future-State Architecture**

    - Define KPIs/KRIs and dashboards for executive reporting.
    - Recommend enterprise-wide security architecture for long-term resilience.
    - Suggest for deployment of Automation tools and Procure Monitoring tools.
    - Making them operation for effective Continuous Monitoring.

B. Managed Security Services

The Managed Security Services (MSS) engagement will provide Continuous and Proactive Technical Security Assurance across the Bank's Technology Environment to Strengthen Cyber Resilience, Validate Security effectiveness, and identify emerging risks and suggest suitable means to monitor the logs and Cyber Security Posture on Continuous basis and pro-actively respond to various Incidents.

Key Deliverables:

- Continuous assessment and validation of the Bank's cybersecurity posture across infrastructure, applications, networks, and digital platforms.
- Review of existing security architecture and identification of security gaps and improvement opportunities.
- Security architecture review and advisory for new business initiatives, systems, and technology implementations.
- Identification and remediation tracking of cybersecurity risks and control gaps.
- Conduct security testing, attack simulation, red teaming exercise and technical assurance activities to validate effectiveness of security controls.
- Assessment and enhancement of security controls aligned with industry standards, regulatory requirements, and best practices.
- Continuous monitoring, reporting, and executive-level visibility of cybersecurity risks and remediation status.
- Delivery of periodic risk assessments, technical assurance reports, and strategic security recommendations.

2. ELIGIBILITY CRITERIA

The Bidder must fulfil following eligibility criteria:

#	Eligibility Criteria for Bidder / OEM	Documents to be submitted	Compliance (Y / N)
GENERAL			
1.	The bidder must be a Registered company under Indian Companies Act. 1956/2013 or LLP/Partnership firm and should have been in existence for a **minimum period of 5 years in India**, as on date of submission of bid.	Copy of the Certificate of Incorporation issued by Registrar of Companies/Registrar of firms and full address of the registered office of the bidder	
2.	The bidder must be registered under G.S.T and/or tax registration in state where bidder has a registered office.	Proof of registration with GSTIN	
FINANCIAL			
3.	The bidder must have minimum average annual turnover **in India of Rs. 500 crores** each year in the last three financial years (i.e. 2023-24, 2024-25,2025-2026).	Copy of Audited Balance Sheet and Certificate of the Chartered Accountant for the last three financial years (i.e. 2023-24, 2024-25,2025-2026)	
4.	The bidder must have made **operating profit in at least two financial years** out of last three financial years (i.e. 2023-24, 2024-25,2025-2026)	Copy of Audited Balance Sheet and Certificate of the Chartered Accountant for the last three financial years (i.e. 2023-24, 2024-25,2025-2026)	
5.	The bidder must have a **positive net worth in last three financial years** (i.e. 2023-24, 2024-25,2025-2026)	Copy of Audited Balance Sheet and Certificate of the Chartered Accountant for the last three financial	

		years (i.e. 2023-24, 2024-25,2025-2026)	
DEFAULT			
6.	At the time of bidding, the Bidder must not have been blacklisted/debarred/ by any Govt. / IBA/RBI/PSU /PSE/ or Banks, Financial institutes for any reason including non-implementation/delivery of the order. Self-declaration to that effect should be submitted along with the technical bid.	Undertaking on Company's letter head	
7.	At the time of bidding, there must not have been any pending litigation or any legal dispute, before any court of law between the Bidder or OEM(if any) and the Bank.	Submit the undertaking self-declaration on Company's letter head	
8.	The bidder must not have NPA with any Bank /financial institutions in India Any case pending or otherwise, with any organization in India which affects the credibility of the Bidder in the opinion of Central Bank of India to service the needs of the Bank may be a ground for rejection of the bid at the discretion of the Bank.	Submit self-declaration on Company's letter head.	
9.	The bidder must have presence in Mumbai and Hyderabad.	Submit the undertaking self-declaration on Bidder's letter head	
10.	If the bidder is from a country which shares a land border with India, the bidder must be	Certified copy of the registration certificate	

	registered with the Competent Authority.		
EXPERIENCE			
11	The bidder must be currently **empanelled with CERT-In** as Information Security Auditing Organization by **10 years**, out of which **last 4 years** should be on continuous basis.	Certificate / Empanelment letter / Equivalent letter issued by Cert-In	
12.	The Bidder must have experience and expertise of each of the service as mention below in at least any one **Schedule Commercial Bank with minimum 2000 Branches in India during last 5 years**. The Project must be of **min. 1 year** duration and of min. **Rs. 2 Lacs value per line item.** 1. Vulnerability Assessment 2. Penetration Testing 3. Web & Application Security 4. Code Review and Secure Coding Practices 5. Mobile Application Security Assessment 6. Red Teaming 7. Digital Forensic Services 8. Regulatory Compliance Review 9. Documentation – Policy, Processes, Procedure	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience.	

	Creation/Review/ Modification etc. **(Minimum one experience in each of the service mentioned above is mandatory)**		
13.	The bidder must **have minimum 70 permanent employees in India** as on date of submission of bids. **Out of 70, min. 20 employees** should mandatorily have either of the • CISA • CISM • CISSP • CRISC • OSCP certification and remaining employees may have any of the below certifications for each employee (Certificate should be in unexpired status and live up to date of submission of bids) • Certified PCI-DSS professional • ISO 27001 LA • ISO 27001 LI • CRTP • CHFI • CIAC • SSCP	Undertaking on bidder letter head needs to submit along with certification details and relevant evidence.	

	• ECSA • CEH Note: The employee having multiple certificates shall be counted one resource only		

***Note:** In case of unaudited Balance Sheet for FY 2025-26, Bidder needs to submit Provisional Balance Sheet along with CA Certificate of Auditor for FY 2025-26.

The bidder must submit only such document as evidence of any fact as required herein. The Bank, if required, may call for additional documents during the evaluation process and the bidder will be bound to provide the same.

Bank reserves the right to verify references provided by the Bidder independently. Any decision of bank in this regard shall be final, conclusive, and binding up on the bidder. Bank may accept or reject an offer without assigning any reason whatsoever.

1. Bidders need to ensure compliance to all the eligibility criteria points.
2. In-case of corporate restructuring the earlier entity's incorporation certificate, financial statements, Credentials, etc. may be considered.
3. In case of business transfer where Bidder has acquired a Business from an entity ("Seller"), work experience credentials of the Seller in relation to the acquired business may be considered.
4. While submitting the bid, the Bidder is required to comply with inter alia the following CVC guidelines detailed in Circular No. 03/01/12 (No.12-02-6 CTE/SPI (I) 2 / 161730 dated 13.01.2012): 'Commission has decided that in all cases of procurement, the following guidelines may be followed:
   - In RFP, either the Indian agent on behalf of the Bidder/OEM or Bidder/OEM itself can bid but both cannot bid simultaneously for the same item/product in the same RFP. The reference of 'item/product' in the CVC guidelines refer to 'the final solution that bidders will deliver to the customer.
   - If an agent submits bid on behalf of the Bidder /OEM, the same agent shall not submit a bid on behalf of another Bidder /OEM in the same RFP for the same item/product.

3. EMD / BID SECURITY

An amount of ₹ 16,00,000/- (Rupees Sixteen Lakh Only) in the form of Bank Guarantee issued by a scheduled bank other than Central Bank of India for the entire period of Bid validity plus 3 months or by means of Account Payee Demand Draft / banker's cheque /RTGS/NEFT in the account no.-3287810289 of Central Bank of India (IFSC Code – CBIN0283154) with narration Tender ref no in favour of "Central Bank Of India" and payable at Mumbai/Navi Mumbai.

The EMD / Bid Security shall be liable to be forfeited:

a) if a Bidder withdraws its tender during the period of tender validity specified by the Bidder; or
b) if the Bidder does not accept the correction of its Tender Price; or
c) if the successful Bidder fails within the specified time to:
   i. Sign the Contract; or
   ii. Furnish the required security deposit.

The EMD / Bid Security of a Joint Venture (JV) must be in the name of the JV that submits the tender. If the JV has not been legally constituted at the time of bidding, the EMD / Bid Security shall be in the names of all future partners as named in the letter of intent.

The EMD / Bid Security will be refunded to The Successful Bidder, only after furnishing an unconditional and irrevocable Performance Bank Guarantee (PBG) as per Clause 4.

The EMD / Bid Security of unsuccessful Bidders shall be returned as promptly as possible after completion of bidding process.

4. PERFORMANCE BANK GUARANTEE

i. As mentioned above, the Successful Bidder will furnish an unconditional and irrevocable Performance Bank Guarantee (PBG) from scheduled commercial Bank other than Central Bank of India, in the format given by the Bank in **Annexure 8**, for 5% of the total project cost valid for 30 months, (2 years for total project period plus 6 months for claim period) validity of PBG starting from its date of issuance. The PBG shall be submitted within 21 days of acknowledgement of the PO by the Bidder.
ii. The PBG so applicable must be duly accompanied by a forwarding letter issued by the issuing bank on the letterhead of the issuing bank. Such forwarding letter shall state that the PBG has been signed by the lawfully constituted authority legally competent to sign and execute such legal instruments. The executor (BG issuing Bank Authorities) is required to mention the Power of Attorney number and date of execution in his / her favour with authorization to sign the documents.
iii. Each page of the PBG must bear the signature and seal of the PBG issuing Bank and PBG number.
iv. In the event of the Successful Bidder being unable to service the contract for whatever reason, Bank may provide a cure period of 30 days and thereafter invoke the PBG, if the bidder is unable to service the contract for whatever reason.
v. In the event of delays by Successful Bidder in AMC support, service beyond the schedules given in the RFP, the Bank may provide a cure period of 30 days and thereafter invoke the PBG, if required.
vi. Notwithstanding and without prejudice to any rights whatsoever of the Bank under the contract in the matter, the proceeds of the PBG shall be payable to Bank as compensation

by the Successful Bidder for its failure to complete its obligations under the contract, indicating the contractual obligation(s) for which the Successful Bidder is in default.

vii. The Bank shall also be entitled to make recoveries from the Successful Bidder's bills or any other amount due to him, the equivalent value of any payment made to him by the bank due to inadvertence, error, collusion, misconstruction or misstatement.

viii. The PBG may be discharged / returned by Bank upon being satisfied that there has been due performance of the obligations of the Successful Bidder under the contract. However, no interest shall be payable on the PBG.

5. Cost of Bidding

The bidder shall bear all the costs associated with the preparation and submission of bid and Bank will in no case be responsible or liable for these costs regardless of the conduct or outcome of the bidding process.

6. Detailed Scope of Work

- The Bidder shall review and study the Bank's existing Cyber Security Setup, Landscape of the Bank which includes Security Architecture, Technology & various Security Tools, Policies, Processes, Security Skill sets etc and then suggest / deliver:

  a. Roadmap - Strategy and execution approach plan outlining proposed methodology, submit detailed implementation and resource deployment plan along with timelines.

  b. Suitable Technologies and Various Security Tools identified through gap assessment activities in line with Regulatory Guidelines/Advisories and Industry Best Practices.

  c. Implement effective and complete Cyber Security Architecture improvement plan. Assist Bank in future proofing security architecture from Quantum attacks and achieve Quantum readiness.

  d. Review and update existing / design and develop new Policies and Processes in line with various frameworks like ISO, Regulatory Frameworks, NIST etc.

  e. Optimize and Tune Bank's Cyber Security tools / solutions including Network Security tools / solutions.

  f. Improved and tuned existing as well as new SCD documents as per the Regulatory Guidelines and Industry Best Practices for OS, DB, Security Devices, Digital Platforms used by the Bank.

  g. Competency mapping, technical skill-gap analysis, and professional certification roadmap for security resources.

  h. Playbook for complete Incident Management framework which includes security escalation matrix for customers, staff, Incident Response and Monitoring Team.

A) Advisory Services

7.1 ISO 27001 & ISO 22301

Bank currently has some of its systems & locations certified with ISO 27001. To advance maturity levels further, Bank wants to further strengthen, enhance, and mature its Information Security Management System (ISMS) and Business Continuity Management System (BCMS) framework in alignment with evolving business, operational, regulatory, and cybersecurity requirements.

The intent of the ISMS in Bank is to define the processes requirement to ensure that risks are identified, appraised to management and addressed in an effective manner. The certification scope of ISO27001 will not be modified, however the recommended and global industry best practices are to be followed across the bank.

The objective of this engagement is to review the existing ISMS and BCMS framework of the Bank, identify gaps and improvement areas, enhance governance and operational effectiveness, and support continual improvement, risk management, compliance management, audit readiness, certification maintenance, and expansion activities in line with ISO 27001:2022, ISO 22301, RBI guidelines, CERT-In advisories, and other applicable regulatory requirements.

The Bidder shall review the existing Cyber Crisis Management Plan (CCMP), Cyber Incident Response framework, escalation procedures, communication matrix, and related cyber security incident handling processes of the Bank. The Bidder shall identify gaps with respect to applicable regulatory requirements, industry best practices, and the Bank's operational environment, and provide suitable recommendations for improvement.

The Bidder shall assist the Bank in preparation, modification, enhancement, and standardization of Cyber Crisis Management Framework, including but not limited to crisis governance structure, roles and responsibilities, escalation hierarchy, incident severity classification, communication and reporting framework, coordination mechanism, regulatory reporting process, and standard operating procedures (SOPs) for handling cyber security incidents.

The Bidder shall also assist the Bank in conducting Cyber Crisis Simulation Exercise / Tabletop Exercise covering various cyber-attack scenarios, response procedures, decision-making process, inter-department coordination, escalation mechanism, and recovery preparedness. Post exercise, the Bidder shall submit detailed observations, gap assessment, corrective action recommendations, and improvement roadmap to the Bank. All activities shall be aligned with

applicable RBI guidelines, CERT-In advisories, NCIIPC recommendations, and industry best practices, wherever applicable.

The key components that need to be put in place as part of ISMS includes

- Risk identification and mitigation planning
- Allocation of responsibility for mitigation
- Status tracking of mitigation
- Management reporting
- Security maturity evaluation over a period of time

Scope of Work:

a) Review the existing ISMS Structure including its roles and responsibilities.
b) Clearly define and combine a risk assessment methodology that is suited to the ISMS standard, and the identified business information security, legal and regulatory requirements.

c) Discuss with the stakeholders and develop criteria for accepting risks and identify the acceptable levels of risk.
d) Interact with key stakeholders and identify all information assets like software assets, databases, records, physical assets, process and service assets, people assets and so on as per ISMS requirement.
e) Evaluate the value of the assets based on business impact after detailed discussions with the stakeholders.
f) Perform Risk Assessment by categorizing the assets by profiling threats, assessing vulnerabilities, analysing impact, and ranking/ prioritizing risks based on the level of threat, level of vulnerability and asset value.
g) Analyse and evaluate the risks based on its business impacts, realistic likelihood of security failures, level of risk and the risk acceptance criteria.
h) Identify and evaluate options for the treatment of risks. Select control objectives and controls for the treatment of risks Present proposed residual risks to management and obtain their buy-in for implementing and operating ISMS.
i) Prepare a Statement of Applicability document
j) Performing Business Impact Analysis (BIA) in a required template for critical business processes (e.g., customer onboarding, loan disbursement, treasury operations)
k) Coordinating with respective process owners to capture key activities impacting the business during BIA process
l) Business process identification, prioritization, or mapping with associated applications.
m) Preparing a final BIA Report
n) Conduct a Risk Assessment based on the BIA on critical processes/activities
o) Assist in implementing security controls (network architecture, access control systems, and secure configuration guidelines etc.).

p) Assist in defining roles and responsibilities of the enforcer, enabler, and auditor; and establish a total compliance program
q) Conduct internal audits with a trained team; drawing up performance metrics; conducting awareness programs among end users; defining processes, roles and responsibilities; ensuring that the Management reviews and works on the Action Plan to close nonconformities (NCs).
r) Develop a framework for periodic risk assessment and mitigation, continual user and IT administrator awareness sessions.
s) Develop a framework for security effectiveness measurement and maintenance of dashboards.

Deliverables:

ISO 27001:

- Controls evidence
- Gap Assessment Report
- ISMS Maturity Assessment Report
- Asset Register
- Risk Assessment Report
- Risk Register
- Risk Treatment Plan (RTP)
- Statement of Applicability (SoA)
- Updated Policies, SOPs, Standards & Guidelines
- Internal Audit Reports
- Compliance & Governance Review Reports
- Security Metrics & Dashboard Framework
- Management Review Reports
- Corrective Action & NC Closure Reports
- Training & Awareness Records
- Audit Readiness & Certification Support Documents
- ISO 27001 Surveillance/Recertification Support
- Review & Gap Assessment Report for existing CCMP and Incident Response Framework
- Updated / Revised Cyber Crisis Management Framework & SOPs
- Cyber Incident Escalation Matrix & Communication Framework
- Corrective Action & Improvement Roadmap Report

ISO22301

- Business Impact Analysis (BIA) Report
- Critical Process Dependency Mapping
- Business Continuity Risk Assessment Report
- Business Continuity Policy & Framework

- RTO/RPO Assessment Report
- Business Continuity Plans (BCP)
- Disaster Recovery Coordination Support
- Crisis Management Framework
- Tabletop Exercise & Mock Drill Reports
- BCMS Audit & Preparedness Reports
- Operational Resilience Review Report
- Corrective Action & Improvement Tracker
- Audit Readiness & Certification Support
- ISO 22301 Surveillance/Recertification Support

Timeline: Annually/As Applicable/As per Bank's Requirement

7.2 ISO 42001 Certification Preparation:

Scope of Work:

The bidder shall provide advisory and implementation support for AI Management System readiness aligned with ISO 42001 requirements. The scope shall include gap assessment, process review and implementation support, policy and procedure development, documentation review, control validation, compliance readiness support and guidance for establishment and improvement related to ISO 42001 certification preparation.

a) Gap Analysis & Discovery:

   i. Evaluation of the current state of AI governance against the ISO/IEC 42001:2023 standard.

   ii. AI Inventory Mapping: Identify all AI use cases. Regulatory Cross-Mapping: Align ISO 42001 requirements with RBI requirements/ MEITY framework and DPDP Act requirements for automated decision-making.

   iii. Gap Assessment: Evaluate existing policies against the applicable controls of ISO 42001.

   iv. Context Definition: Define the internal and external issues, and the scope of the AI related systems.

b) AI Framework Design & Documentation:

   i. Draft a high-level AI Policy and Statement of Applicability (SoA).

   ii. Governance Structure: Define roles like "AI Risk Officer" or "AI Ethics Committee" and their reporting lines to the Board.

   iii. Risk Management Framework: Design an AI-specific risk assessment process

iv. AI System Impact Assessment Templates: Create standardized forms to evaluate the impact on stakeholders (fairness, transparency, and accountability).

C) Technical Controls & Implementation Support: Practical application of the standard to the bank's technical environment.

i. Data Governance for AI: Establish controls for data lineage, quality, and provenance for training/tuning datasets.

ii. Lifecycle Management: Implement controls for the AI lifecycle

iii. Transparency & Explainability: Define technical requirements for "Model Explainability" to ensure the bank can justify automated credit or fraud decisions to regulators.

iv. Human Oversight: Design workflows for human intervention in high-risk AI outputs.

D) Security & Robustness Integration:

a) Adversarial Threat Modelling: Assess risks like prompt injection, data poisoning, and model inversion.

b) Incident Response: Update the bank's Incident Response Plan to include AI-specific failure modes (e.g., mass-misinformation or algorithmic bias incidents).

c) Third-Party AI Risk: Establish due diligence checklists for vendor-provided AI models (SaaS or API-based).

E) Readiness Review & Pre-Audit:

a) Internal Audit: Conduct a full "mock" audit.

b) Competency & Training: Conduct awareness sessions for bank staff and specialized training for the AI development and compliance teams.

c) Management Review Support: Prepare the documentation for the "Management Review Meeting" (MRM) to ensure top-level leadership sign-off.

d) Certification Body Selection: Assist in selecting an accredited Registrar and coordinating the Stage 1 and Stage 2 audits.

Deliverables:

- Gap analysis report; AI system inventory; Initial risk/impact assessment.
- AI policies; Risk treatment plan; AI system impact assessments (societal/ethical risks).

- Control evidence (bias checks, data lineage); Staff competence records; Operational AIMS.
- Internal audit report; Management review minutes; non-conformity closure.
- Stage 1/2 audit support; Readiness report for; ISO 42001 certificate.

Timeline: Annually/As Applicable/As per Bank's Requirement

7.3 Cyber Security Tools/solutions including Network Security Tools/solutions Configuration and Assessment

The bidder shall assess configuration, effectiveness and operational coverage of deployed cyber security tools/solutions including network security tools/solutions of the Bank. The review shall not be limited to policies, rules, signatures, alerts, logging and monitoring configurations across security technologies.

Scope of Work:

Conduct comprehensive configuration review, optimization, tuning of Bank's cyber security tools/solutions including network security tools/solutions as per RBI NIST and MITRE ATT&CK framework requirement.

A) Assessment of Data Ingestion & Normalization: Source coverage of critical logs like CBS/UPI/ATM/AD / SWIFT etc., Log retention, Time synchronization, Parsing rules, Index optimization etc.
B) Assessment of Detection Rules like Authentication, Database changes, Network Port scans, lateral movements, SMB/RDP etc, validation of rules at Bank defined frequency.
C) Assessment of Alerting & Correlation: MTTD targets, Correlation rules from Multi-source like EDR, FW, SIEM etc.
D) Assessment of False positives tuning, Critical incident detection SLA, SOC maturity etc.
E) Assessment of Endpoint Coverage in EDR, Behavioural analytics, Response capabilities, etc
F) Assessment of Firewalls / NG-Firewalls configuration: Rule based optimization, Bank specific policies, Threat Prevention capabilities.
G) WAF configuration assessment: Internet facing applications, rules review, coverage etc.
H) Assessment of Cyber Security Tools/Solutions including Network Security Tools/Solutions, configuration, rules, alerting, maturity etc.
I) Assessment of integration of various cyber security tools including network security with SOC and its effectiveness as per MITRE ATT&CK and NIST framework.
J) Assessment of various dashboards / management visibility / holistic view.

Deliverables:

- Current state assessment report
- Use case and detection review report
- Gap analysis and SOC maturity report
- Optimization and tuning recommendations
- Post-implementation validation report

Timelines: Half Yearly/As Applicable/As per Bank's Requirement

7.4 Red Teaming:

Scope of Work:

- The Bidder shall perform Red Teaming and adversary simulation exercises based on the MITRE ATT&CK framework, industry best practices and evolving threat landscape relevant to the banking sector. The scope shall include mapping of attack vectors, tactics, techniques and procedures (TTPs), validation of detection and response capabilities, identification of monitoring gaps and submission of detailed observations with mitigation recommendations.
- The bidder shall carry out Red Teaming / adversary simulation exercises in a controlled and pre-approved manner to assess the Bank's preparedness for detecting, responding to, containing, and recovering from sophisticated cyber-attacks targeting the Bank's infrastructure, applications, users, and critical business environments.
- The Red Teaming exercise shall be aligned with the MITRE ATT&CK framework, industry best practices, evolving threat landscape, and banking sector-specific attack scenarios. The scope shall include simulation of attack vectors, tactics, techniques, and procedures (TTPs), assessment of monitoring and detection effectiveness, validation of response capabilities, identification of security gaps, and submission of detailed observations along with mitigation recommendations.
- The bidder shall coordinate closely with the Bank for defining scope, rules of engagement, execution windows, escalation procedures, communication mechanisms, approvals, reporting structure, and operational safeguards prior to commencement of Red Teaming activities.
- The bidder shall ensure that all Red Teaming activities are conducted in a controlled, authorized, and non-disruptive manner without causing adverse impact on production systems, business operations, data integrity, customer services, or critical infrastructure of the Bank.
- The bidder shall provision, manage, and utilize all required tools, frameworks, utilities, software, licenses, payload simulation mechanisms, phishing simulation platforms, command-and-control (C2) infrastructure, reporting utilities, and supporting resources

required for execution of Red Teaming activities under the scope of work, without any additional cost to the Bank unless specifically approved otherwise by the Bank.

- The bidder may utilize industry-standard commercial and/or open-source tools, frameworks, and utilities required for execution of Red Teaming activities, subject to prior approval of the Bank, defined scope, controlled execution methodology, security safeguards, logging requirements, and compliance with the Bank's security policies, regulatory/advisory requirements, and applicable laws.
- The bidder shall maintain complete inventory and documentation of all tools, payloads, frameworks, scripts, and utilities utilized during the engagement and ensure secure cleanup/removal of the same upon completion of activities.
- Usage of destructive payloads, live malware, unauthorized persistence mechanisms, uncontrolled command-and-control infrastructure, or activities causing operational disruption shall not be permitted unless explicitly approved by the Bank in writing.
- Reconnaissance & Initial Access Simulation including Spear-Phishing, OSINT harvesting, Vishing (Voice Phishing), Watering Hole attacks, credential harvesting, and external attack surface analysis.
- Execution, Evasion & Persistence Testing targeting endpoints, servers, and user environments including defence evasion techniques, persistence validation, MFA bypass simulation, and endpoint security control effectiveness assessment.
- Privilege Escalation & Lateral Movement Simulation across internal network environments to assess segmentation effectiveness, monitoring capabilities, and detection mechanisms.

  Note: AD is the backbone of Indian banks. This is where most time should be spent.

- Active Directory (AD) Compromise Simulation including Kerberoasting, AS-REP Roasting, Pass-the-Hash, Golden Ticket simulation, privilege abuse scenarios, and identity-based attack path analysis.
- Targeting critical applications: Core Banking System, Digital Payments Infrastructure, Targeting internal APIs, SWIFT Environment etc.
- Data Exfiltration Simulation: Testing Data Loss Prevention (DLP) and Network Traffic Analysis (NTA) by attempting to tunnel simulated data out via DNS, HTTPS, or ICMP.
- Impact & Resilience Assessment including validation of backup security controls, incident response readiness, containment capabilities, and operational resilience measures.
- Controlled Ransomware Simulation using benign and non-destructive payload mechanisms for assessing detection speed, response coordination, containment effectiveness, backup integrity validation, and recovery preparedness.

- Validation of detection and response capabilities through MITRE ATT&CK mapping, attack path analysis, monitoring gap identification, and adversary behaviour simulation.

- Security Monitoring & Detection Validation to assess effectiveness of SOC monitoring, SIEM correlation rules, alert generation, threat detection coverage, incident escalation, and response coordination mechanisms.

- Conduct AI-led Read teaming and simulate AI based attacks in the red teaming in the applicable environment in consultation with Bank. Successful bidder to bring in the tools required for this activity at their own cost, if required.

Deliverables:

- Red Team Strategy, Methodology & Rules of Engagement Document
- Red Team Scenarios & Attack Simulation Plan
- Reconnaissance & Attack Surface Assessment Report
- Attack Path / Kill Chain Analysis Report
- Active Directory Security Assessment Report
- MITRE ATT&CK Mapping & Coverage Assessment Report
- SOC Detection & Monitoring Gap Assessment Report

- Incident Response & Containment Effectiveness Review Report
- Data Exfiltration & DLP Validation Report
- Critical Application Attack Simulation Report
- Security Control Effectiveness Assessment Report
- Detailed Red Team Findings & Risk Assessment Report
- Risk Mitigation & Remediation Recommendations Report
- Re-testing / Validation Report
- Executive Summary & Management Presentation Report
- Tool, Framework & Payload Inventory Documentation
- Final Closure & Cleanup Confirmation Report

Timelines: Quarterly/As Applicable/As per Bank's Requirement

7.5 Security and Network Architecture Review

Scope of Work:

The bidder shall review the Bank's existing network, infrastructure and security architecture to identify design gaps, security weaknesses and improvement opportunities. The review shall include DC, DR, branch connectivity, network connectivity from branch office to DC and DR, perimeter security and critical security infrastructure components, and ATM networks. The scope shall also include review and advisory support for proposed and upcoming projects,

network/security architecture planning, security standards, policies, procedures, hardening guidelines, implementation guidelines and related documentation to ensure alignment with industry best practices, regulatory requirements and future security readiness of the Bank.

- Review for Network security architecture
- Review the appropriate segregation of network into various trusted zones
- Review the traffic flow in the network
- Review of routing protocols and security controls therein
- Review the security measures at the entry and exit points of the network
- SOC/ C-SOC Architecture review
- Configuration review of network and security devices including Firewall, IPS, IDS, Routers, Switches, etc.
- Rule based review of firewall and IPS
- Review of security measures at entry and exit points of network
- Review of key processes related to network and information security
- Network vulnerability assessment
- Review Cyber Security Architecture from Quantum Readiness perspective and to combat against Quantum Attacks.
    a) Comprehensive Asset Discovery & Post Quantum Cryptography (PQC) Readiness Audit
    b) Cryptographic Agility Strategy & Target Architecture Design
    c) Hybrid Security Models & Quantum Key Distribution (QKD) Implementation Blueprints

Deliverables:

- Assessment methodology
- Detailed assessment report including recommendations (quick fix, short fix, etc.)
- Action Plan for closure of reported findings
- Detailed closure report
- Executive summary report
- Comprehensive Cryptographic Asset Inventory Report
- Cryptographic Agility Architecture Blueprint Document.
- Fully Configured Hybrid Encryption Test Environment.
- Final Quantum Transition Validation and Performance Report.

Timelines: Half Yearly/As Applicable/As per Bank's Requirement

7.6 Secure Configuration documentation and reviews

The bidder shall prepare, review and validate secure configuration standards and hardening guidelines for servers, databases, operating systems, applications and security devices. The

activity shall include configuration review against industry best practices and regulatory guidelines.

Scope of work:

- Designing of new SCDs or modifying the existing SCDs for operating systems/databases / security devices/ Digital platforms used in bank, as per the industry best practice / regulatory guidelines with necessary customization for bank and not limited to CIS benchmarks.
- Providing recommendations / support to Bank in implementation of these SCDs

Deliverables:

- Successful Bidder has to provide the Hardcopy and softcopy of SCD documents and scripts.
- All SCDs should be controlled with version no., maker, and reviewer etc. as per best practice.
- Every control configuration setting should be with detailed description and not limited to objective, impact, severity, solutions, steps for setting, etc.

Timelines: Half Yearly/As Applicable/As per Bank's Requirement

7.7 AI Technology Vulnerability Management

Scope of Work:

The bidder shall assess AI based systems, Large Language Model (LLM) based technologies, and related AI technologies for identification of emerging cyber security risks and vulnerabilities. The scope shall include review of AI security controls, risks, prompt injection risks, data leakage risks, unauthorized access risks, model manipulation threats, and governance and compliance related concerns associated with AI technologies.

A. Assessment of model security risks, data pipeline risks, API security risks, API and infrastructure risks etc.

B. AI specific technologies assessment shall not be limited to Fraud detection systems, Credit scoring models, Chatbots etc.

Deliverables:

- AI / ML security assessment scope note
- AI security analysis report
- Final report with mitigation plan

- Validation report

Timelines: Quarterly/As Applicable/As per Bank's Requirement

7.8 Cyber Security Maturity Assessment

The bidder shall conduct cyber security maturity assessment across people, process and technology domains of the Bank. The assessment shall include identification of maturity gaps and submission of roadmap recommendations for improvement and enhancement.

Scope of Work

- Asses present cyber security maturity level of the Bank.
- Provide an industry standard model consisting of but not limited to following 10 domains, to enable Bank to regularly assess its own Cyber Maturity level:
- Governance, Risk & Compliance (GRC)
- Asset Management
- Identity & Access Management (IAM)
- Network & Infrastructure Security
- Security Operations & Monitoring
- Application Security
- Data Security & Privacy
- Cloud Security
- Incident Response & Cyber Resilience
- Security Awareness & Training

Assessment Methodology

The bidder shall adopt a recognized cybersecurity maturity framework, including but not limited to:

- NIST Cybersecurity Framework
- ISO/IEC 27001
- CIS Controls

Deliverables

- Project kick-off and assessment plan
- Current-state documentation review
- Stakeholder interviews and workshops
- Cyber maturity assessment across domains

- Gap analysis and findings register
- Benchmarking and target maturity model
- Remediation roadmap and action plan
- Final assessment report
- Executive presentation
- Closure and knowledge transfer
- Heatmaps and dashboards
- Comparative maturity analysis
- Benchmarking observations
-

Timeline: Annually/As Applicable/As per Bank's Requirement

7.9 KRI / KPI reviews

Scope of Work:

The bidder shall review cyber security related Key Risk Indicators (KRIs), and Key Performance Indicators (KPIs) implemented within the Bank. The activity shall include assessment of monitoring effectiveness, reporting mechanisms and alignment with regulatory and operational requirements. The bidder shall analyse the existing KRIs/KPIs and provide suitable recommendations for inclusion of relevant controls, monitoring parameters, checkpoints, and reporting requirements within the Bank's IS Audit framework.

- Assess the IT GRC implementation by the Bank, review existing KPIs / KRIs
- Formulate new /existing KRIs / KPIs as per National Cyber Security Reporting Framework (NCRF) / Regulatory Framework
- Identify gaps with reference to industry best practices/regulatory compliance
- Assist Bank in fulfilling the gaps & formulating new KPIs/KRIs and/modify existing KPIs / KRIs.
- Assist Bank in modification/ updation in IS audit framework as per KPIs / KRIs
- Provide final review of the compliance

Deliverables:

- KPI / KRI definition document
- Recommendations for inclusion in IS Audit

- Dashboard design / framework note
- Implementation support / review note
- Final dashboard / final review report
- Validation report

Timeline: Quarterly/As Applicable/As per Bank's Requirement

7.10 Regulatory Compliance Review

- Reserve Bank of India (RBI) issues circulars, advisories and alerts & Master directions on cyber security regularly and directs Banks to implement the directions & recommendations suggested in the circulars, advisories & Alerts. In addition, Bank also receives such circulars, advisories and alerts on cyber security from CERT-in, NCIIPC, IB-Cart, MeitY, GOI, IFSCA and other regulatory agencies. Also, regulatory audits like IT Examination are conducted in periodic manner. Bidder is expected to review the onsite implementation of the RBI Alerts, advisories, audit gaps, IT Examination gaps. Also, assist Bank in Defending Technology Stacks Against AI-Accelerated Cyber Threats and AI Governance and Security Framework.

Scope of work:

- Review of all advisories, alerts and circulars since 2016 till date of submission of final report.
- Collection of evidence against each line item of RBI Guidelines (Advisory, Alert & Circular), NCIIPC Guidelines for Critical Information Infrastructure (CII) and advisory digest.
- carry out a gap assessment in the light of the above requirements and frame a time bound action plan with the approval of Board / IT Strategy Committee/ Risk Management Committee of Board, as the case may be, within a time period of two months to enhance their processes and capacities accordingly.
- Carry out a gap assessment frame a time bound action plan as the case may be, within a limited time period to enhance their processes and capacities accordingly.
- Validation of evidence/ supporting documents for the complied observations / directions.
- Physical / Technical verification of compliance submitted by concerned teams in the systems / devices and report the actual implementation status.
- Review of procedures followed by the departments, with guidelines issued by RBI.
- Review of adequacy of existing processes being followed, systems/tools being deployed with respect to RBI directions and identify gaps, if any.
- Assist Bank to comply with various frameworks, advisories, audits etc issued by the Regulators within timelines.

- Risk Assessment and Preparedness.
- Architecture and Cyber Resilience
- Vulnerability and Patch Management
- Monitoring, Detection, Response and Testing
- AI-Enabled Social Engineering and Impersonation
- Leveraging AI Tools for Cybersecurity / IT activities
- AI Governance
- Classification, Ownership and Lifecycle Management
- Secure Development, Integration and Configuration
- Access Control and Data Protection
- AI Specific Threat Controls
- Performance Monitoring and Output Validation
- AI Change Management
- Logging, Traceability and Forensic Readiness
- Resilience and continuity
- AI Agents and Privilege Access
- Third Party AI Risk Management
- AI Usage Policy and Controls
- Audit, Testing, Training and Awareness

Deliverables:

- Project initiation and assessment plan
- Current-state review and evidence collection
- Stakeholder interviews and workshops
- Cyber maturity assessment report by domain
- Gap analysis and risk findings
- Target maturity model / benchmark
- Remediation roadmap
- Final assessment report
- Management presentation / closure meeting
- Knowledge transfer and handover

Timeline: Half Yearly/As Applicable/As per Bank's Requirement

7.11 Documentation – Policy, Processes, Procedure Creation/Review/ Modification etc.

The bidder shall review, prepare and enhance Cyber Security related policies, standards, processes, procedures, SOPs and operational documents of the Bank. The activity shall ensure alignment with regulatory guidelines, industry standards and operational requirements of the Bank.

Scope of Work

- Drafting new Policy, Processes, Procedure for Bank as per Bank/ Regulatory requirement
- Vendor to identify gaps in already defined policies/procedures of the Bank. Help Bank in filling these gaps with industry best practices /regulatory guidelines
- Provide assistance to Bank in complying / fulfilling these gaps

Deliverables

- GAP Assessment Report
- Policy Documentation (New/Revised)
- Process Documentation
- Standard Operating Procedures (SOPs), guidelines and standards
- Regulatory Compliance Mapping Document
- Gap Closure Action Plan
- Policy Review & Modification Log
- Final Compliance Report

Timeline: Half Yearly/As Applicable/As per Bank's Requirement

7.12 SOC Review

The bidder shall assess the effectiveness of Security Operations Centre (SOC), SIEM monitoring, incident management and security monitoring processes of the Bank. The review shall include use case assessment, alert effectiveness, log monitoring and incident response capabilities.

Scope of Work:

1. SOC Governance & Maturity Assessment: The consultant must evaluate the foundational operational health of the SOC.

- People & Skills Audit: Assess the competency levels of Tier 1, 2, and 3 analysts. Evaluate the bank's internal vs. Outsourced responsibility matrix.
- Process Maturity (SOC-CMM): Audit Standard Operating Procedures (SOPs) for the incident lifecycle.
- Technology Stack Review: Evaluate the efficiency and integration of the SIEM, SOAR, EDR/XDR, Threat Intelligence Platform (TIP), other cyber security tools/solutions including network security tools/solutions.
- Compliance Alignment: Ensure SOC operations align with RBI CSITE requirements, including log retention and incident reporting timelines.
- Threat Hunting Maturity

2. MITRE ATT&CK Mapping & Gap Analysis

- Log Source & Visibility Mapping: Identify if the bank is collecting the right telemetry required to detect MITRE techniques.
- Detection Rule Mapping: Map the bank's existing SIEM correlation rules, EDR alerts etc to the MITRE ATT&CK Matrix
- Tactical Gap Identification: Identify "Blind Spots." for example if the SOC can detect *Lateral Movement* or *Credential Access* beyond simple brute-force alerts.
- Threat Prioritization: Focus the matrix on threats specific to the Indian financial sector, such as Ransomware-as-a-Service (RaaS) and APTs targeting critical systems etc.

3. Active Detection Validation

- Adversary Emulation: Conduct controlled, non-disruptive "Atomic Tests" to emulate specific MITRE techniques.
- Efficacy Testing: Verify if the SIEM/EDR other tools triggered an alert during emulation and evaluate the Mean Time to Detect (MTTD).
- Alert Fatigue Analysis: Evaluate the ratio of True Positives to False Positives.

4. Incident Response & Playbook Review

- Review of existing Incident Response mechanism and suggest action plan for any gaps found
- Playbook Assessment: Review SOAR (Security Orchestration, Automation, and Response) playbooks.
- Communication Flow: Assess the escalation matrix.
- Forensic Readiness: Evaluate the SOC's ability to preserve evidence and perform root-cause analysis without disrupting bank operations.

Deliverables:

- SOC Governance & Maturity Assessment Report
- Threat Hunting Maturity Report
- MITRE ATT&CK Mapping & Gap Analysis Report
- Active Detection Validation Report

- Incident Response & Playbook Assessment Report
- Forensic Readiness & Final SOC Review Report
- Final Closure Report

Timelines: Half Yearly/As Applicable/As per Bank's Requirement

7.13 Cyber Resilience Preparedness:

Scope of Work:

The bidder shall assess the Bank's preparedness to prevent, withstand, respond to and recover from cyber security incidents and operational disruptions. The activity shall include review of resilience mechanisms, response processes and recovery preparedness capabilities.

The bidder shall design, develop, and establish the framework, methodology, governance structure, SOPs, operational procedures, communication flow, escalation matrix, stakeholder responsibilities, and reporting mechanisms for conducting Tabletop Exercises (TTX) related to cyber incidents, business continuity, disaster recovery, and operational resilience scenarios within the Bank.

- Resilience Framework Benchmarking: Evaluate the bank's current posture against ISO standards and Regulatory frameworks requirements to establish a baseline.
- Prevention Capability Audit: Review the effectiveness of proactive controls (e.g., Threat Intel, Zero Trust architecture etc) intended to prevent the initial success of a cyber-threat.
- Critical Business Operations / Processes Mapping: Identify services that must remain available (e.g., CBS, UPI, Swift, RTGS etc) and define their "Maximum Tolerable Downtime" to ensure the bank can absorb impact.
- Red Teaming & Adversarial Simulations: Execute simulations to see if the bank can prevent any breach without a total collapse of critical banking workflows.
- Technical Dependency Analysis: Map the interconnections between internal systems and third-party FinTech / Cloud providers to identify hidden vulnerabilities in the response chain.
- Incident Response Mechanism Review: Enhance the bank's ability to respond rapidly incidents, to meet regulatory requirement and to ensure that the containment is effective.
- Tabletop Exercises: Facilitate crisis simulations to test the ability to respond during a cyber-outage.
- Recovery Time (RTO) & Point (RPO) Validation: Validate the technical ability to recover data and systems within the strict timelines mandated by the RBI for critical banking services.
- Immutable Backup & Air-Gap Review: Evaluate the integrity of off-line or immutable backups, ensuring they are available to recover from destructive attacks including Ransomware.
- Clean-Room Recovery Planning: Develop a strategy to recover and validate systems in an isolated environment before reconnecting them to the live production network.
- Regulatory Reporting Readiness: Ensure the bank is ready to respond to regulators within the prescribed timeline and comply with various regulatory requirements.

- Post-Incident Adaptability: Establish a framework to improve the readiness by integrating lessons learnt from simulations and recovery planning into future defences.
- The bidder shall design, develop, and establish the framework, methodology, governance structure, SOPs, operational procedures, communication flow, escalation matrix, stakeholder responsibilities, and reporting mechanisms for conducting Tabletop Exercises (TTX) related to cyber incidents, business continuity, disaster recovery, and operational resilience scenarios within the Bank.

Deliverables:

- Resilience Framework Benchmarking Report
- Prevention Capability Audit Report
- Critical Business Operations Mapping Report
- Technical Dependency Analysis Report
- Red Teaming & Adversarial Simulation Report
- Incident Response Mechanism Review Report
- Tabletop Exercise Report
- RTO & RPO Validation Report
- Immutable Backup & Air-Gap Review Report
- Clean-Room Recovery Plan
- Regulatory Reporting Readiness Report
- Post-Incident Adaptability Framework
- Final Cyber Resilience Report
- Tabletop Exercise (TTX) Framework, Governance & Operational Document & Preparedness
- Scenario-Based TTX Methodology & Workflow Document
- TTX SOPs, Operational Procedures & Guidelines, Roles & Responsibilities Matrix
- TTX Observation, Reporting & Documentation Templates
- Response Coordination & Decision-Making Framework
- Lessons Learned & Improvement Tracking Framework
- Final TTX Readiness & Framework Establishment Report

Timelines: Half Yearly/As Applicable/As per Bank's Requirement

7.14 ISD Resource Assessment and Future Resource Planning

Scope of Work:

- The bidder shall assess the existing Information Security Department (ISD) and associated IT/Cyber Security resource ecosystem of the Bank, including current manpower deployment, roles and responsibilities, skill sets, operational capabilities, and resource utilization. The bidder shall perform a detailed gap assessment with respect to the Bank's existing and future business, technology, regulatory, operational, and cyber security requirements. Based on the assessment, the bidder shall provide recommendations on future resource planning, including proposed manpower strength, role categorization, required skill sets, certifications, domain expertise, operating

model, and resource deployment strategy required for effective management and strengthening of the Bank's IT and Cyber Security ecosystem.

- The Bidder shall review the Bank's existing cybersecurity capabilities and provide suitable recommendations for establishment and strengthening of a dedicated team focused on advanced cybersecurity technologies, emerging cyber threats, threat intelligence, and evolving attack vectors.

- The bidder shall also recommend an appropriate operational model, skill requirements, training framework, technology adoption approach, and capability development roadmap to build necessary in-house competency and dependency within the Bank for proactive identification, analysis, mitigation, and management of advanced and emerging cyber threats.

- Further, the bidder shall suggest mechanisms for continuous research, technology evaluation, cyber threat monitoring, knowledge enhancement, and integration of industry best practices to strengthen the Bank's preparedness against evolving cybersecurity risks and future threat landscape.

- The bidder shall develop and recommend comprehensive Standard Operating Procedures (SOPs), operational workflows, incident response procedures, monitoring guidelines, and governance mechanisms for cybersecurity operations within the Bank. The bidder shall also conduct knowledge transfer sessions and provide necessary training to the Bank's personnel for effective implementation, operational handling, and continuous improvement of cybersecurity processes and controls.

- Further, the bidder shall define cybersecurity benchmarks, Key Performance Indicators (KPIs), Key Risk Indicators (KRIs), measurable metrics, and centralized dashboards for continuous monitoring, performance assessment, risk visibility, and management reporting. The dashboards and reporting framework shall enable effective tracking of security posture, incident trends, compliance status, operational efficiency, and remediation activities.

- The bidder shall also establish and recommend structured monitoring and response SOPs covering key cybersecurity domains including but not limited to perimeter security, network architecture security, endpoint and server security, application security, vulnerability and threat management, Security Operations Centre (SOC) operations, red team assessment and adversarial simulation activities, incident response, log monitoring, and cyber threat intelligence management to ensure proactive and continuous cybersecurity monitoring across the Bank's environment.

- The Bidder shall also support the Bank in establishment, enhancement and operationalization of Blue Team and Purple Team capabilities for proactive threat detection, attack simulation validation, incident response improvement and security monitoring enhancement. The scope shall include coordination between Red Team and SOC/Blue Team functions, validation of detection and response use cases, adversary simulation exercises, detection gap identification, threat hunting support, playbook enhancement, process improvement recommendations and knowledge transfer activities for strengthening the Bank's cyber defence capabilities. The bidder shall assist, guide, and support the Bank in establishing and strengthening internal Blue Team and Purple Team capabilities, including defining operational framework, roles and responsibilities, monitoring processes, threat detection and response procedures, coordination mechanisms, skill enhancement roadmap, SOPs/playbooks, and alignment with industry best practices and frameworks such as MITRE ATT&CK.

The scope of work shall include, but not be limited to, the following activities:

a) Current State Assessment

The bidder shall perform assessment of the existing ISD and related IT/Cyber Security operational ecosystem of the Bank, including:

- Existing organizational structure of ISD and associated teams.
- Current manpower deployment across various security and IT functions.
- Existing roles, responsibilities, reporting hierarchy, and operational dependencies.
- Assessment of resource allocation, utilization, productivity, and operational efficiency.
- Review of existing capabilities in areas such as SOC operations, incident response, vulnerability management, governance, compliance, risk management, network security, application security, endpoint security, cloud security, SIEM operations, and related functions.
- Review of current support model involving internal teams, OEMs, System Integrators (SI), Managed Security Service Providers (MSSP), and other third-party stakeholders.
- Assessment of skill gaps, dependency risks, single points of failure, and operational limitations.

b) Gap Assessment

The bidder shall carry out a detailed gap assessment of the existing ISD ecosystem against:

- Regulatory and compliance requirements issued by RBI, CERT-In, NCIIPC, NPCI, IFSCA and other applicable authorities.
- Industry best practices and cyber security frameworks.
- Existing and future business requirements of the Bank.
- Technology landscape, digital transformation initiatives, and critical infrastructure requirements.

- Existing security monitoring, governance, operational, and incident management capabilities.

The bidder shall identify gaps in:

- Manpower strength and resource availability.
- Skill sets and competency levels.
- Role segregation and accountability structure.
- Operational coverage and shift management.
- Security monitoring and response capabilities.
- Governance and compliance management.
- Technology management and specialized security functions.

c) Future Resource Planning and Operating Model

Based on the assessment findings, the bidder shall recommend a future-state resource and operational model for the Bank, including:

- Recommended organizational structure for ISD and associated cyber security functions.
- Proposed manpower planning and resource estimation.
- Recommended role-wise resource categorization.
- Required technical skill sets, certifications, and domain expertise for each role.
- Resource deployment model for DC, DR, SOC, branches, and centralized operations, wherever applicable.
- Proposed L1, L2, L3 and specialized security resource structure, wherever applicable.
- Recommendations for shift-based operations, 24x7 monitoring requirements, escalation matrix, and operational governance.
- Recommendations on outsourcing, co-sourcing, FMS, managed services, or hybrid operational models, wherever applicable.
- Succession planning, cross-skilling, and capability enhancement recommendations.

d) Strategy, Roadmap and Implementation Planning

The bidder shall prepare and submit:

- Detailed strategy document for strengthening the ISD and cyber security operational ecosystem.
- Phase-wise implementation roadmap and execution plan.
- Prioritized action plan for closure of identified gaps.
- Timeline and milestone-based implementation approach.
- Dependency analysis and implementation considerations.
- Recommendations for short-term, medium-term, and long-term resource and operational enhancement.

e) Deliverables

The bidder shall submit, at minimum, the following deliverables:

- Current State Assessment Report.
- ISD Gap Assessment Report.
- Resource Skill Gap and Competency Assessment Report.
- Future Resource Planning and Organization Structure Report.
- Role-wise Skill Set and Certification Recommendation Matrix.
- Resource Deployment and Operating Model Recommendation Report.
- Implementation Strategy and Roadmap Document.
- Final Presentation to Senior Management / Project Monitoring Committee.
- Final Closure and Recommendation Report.

f) Deliverables for Blue Team and Purple Team formation

- Blue Team & Purple Team Formation & Capability Development Assessment Report of Existing Cyber Security Operations and Security Monitoring Capabilities
- Gap Assessment Report for Internal Blue Team and Purple Team Readiness
- Blue Team Formation & Operationalization Framework Document
- Purple Team Collaboration & Engagement Framework Document
- Roles & Responsibilities Matrix for Blue Team and Purple Team Members
- Organization Structure & Resource Planning Recommendations for Cyber Defence Teams
- Skillset, Certification & Competency Requirement Matrix for Proposed Teams
- SOPs, Playbooks, Escalation Matrix & Operational Guidelines for Security Operations
- Threat Monitoring, Incident Response & Threat Hunting Framework Recommendations
- MITRE ATT&CK Alignment & Cyber Defence Capability Mapping Report
- Security Operations Governance & Reporting Framework
- KPI/KRI & Operational Dashboard Recommendation Framework
- Training, Awareness & Knowledge Transfer Sessions for Internal Teams
- Tabletop Exercise & Purple Team Coordination Exercise Reports
- Cyber Défense Maturity Improvement & Capability Enhancement Roadmap
- Strategic Recommendations for Continuous Monitoring, Detection & Response Improvement
- Final Blue Team & Purple Team Readiness and Implementation Recommendation Report

f) Validation and Review

The bidder shall conduct review sessions and walkthroughs with the Bank's designated officials and incorporate observations/comments provided by the Bank before final submission of deliverables.

Timelines: One Time Activity/As Applicable/As per Bank's Requirement

B) Managed Security Services

7.15 Vulnerability Assessment

Scope of Work

The bidder shall perform vulnerability assessment of servers, endpoints, databases, operating systems, network devices and other critical IT assets of the Bank. The activity shall include identification, classification and reporting of security vulnerabilities along with risk rating and remediation recommendations.

- Bank expects an authenticated type but non-destructive vulnerability assessment to be carried out.
- The Security review should cover comprehensive assessment of technological, functional; processes associated with the systems and IT/Digital and Information and Cyber Security eco system associated with systems under the scope of such review. Vendors are expected to conduct the audit against the standard configuration document that bank has created, as also the latest global standards and industry best practices. In case, any new asset is identified during project execution, vendor is expected to develop the checklist and conduct the assessment.
- The purpose of the vulnerability assessment is to discover all systems on perimeter network or internet facing and to assess these systems for securities vulnerabilities. Vulnerability assessment shall attempt to determine vulnerabilities that may enable unauthorized logical access to protected system via the external network interfaces by a 'naive' intruder who has limited and/ or no previous knowledge of the Bank's network. The vendor will conduct vulnerability assessment against network and security infrastructure components to identify services in use and potential vulnerabilities present.
- The assessment should check for various categories of threats including:

    a. Unauthorized access into the network and extent of such access possible
    b. Unauthorized modifications to the network and traffic flowing over network
    c. Extent of information disclosure from the network
    d. Spoofing of identity over the network
    e. Possibility of denial of services
    f. Possible threats from malicious codes (viruses and worms etc.)
    g. Possibility of traffic route poisoning

- General aspects for all systems

a. Access control and authentication
b. Network settings
c. General system configuration
d. Logging and Auditing
e. Password and account policies

f. Patches and Updates

- Specific requirements for Server/OS Configuration Audit

a. File system security
b. Account Policies
c. Access Control
d. Network Settings / Network Port / Network Access Details
e. System Authentication
f. Logging and Auditing
g. Patches and Updates
h. Unnecessary services
i. Remote login settings

- Configuration Audit of Networking & Security Devices

a. Access Control
b. System Authentication
c. Auditing and Logging
d. Insecure Dynamic Routing Configuration
e. Insecure Service Configuration
f. Insecure TCP/IP Parameters
g. System Insecurities
h. Unnecessary services
i. Remote login settings
j. Latest software version and patches
k. Traffic Analysis

- Database Configuration Audit

a. Database Account Authentication
b. Password Policy
c. Database Account Privileges
d. Database Auditing
e. Database Logging and Tracing
f. Database Network Access Mechanism
g. Database Patching
h. Database Files and Directories Permission
i. Access control and authentication
j. Unnecessary services
k. Remote login settings
l. Patches and updates

- Security configuration of desktops, laptops, tablet phones and mobile devices that are used by the business users can be performed on sampling basis as per Bank's requirements.

- API Security :

a. API Inventory: Identify and document all APIs (REST, SOAP, GraphQL, etc.)
b. Vulnerability Testing:SQL injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), API injection attacks, Broken authentication and session management etc.
c. API Configuration Review: API gateway configuration, Security headers and policies, Logging and monitoring.

Deliverables :

- Scope finalization, target confirmation and test plan
- Penetration Testing Report
- Final Consolidated Report
- Post-remediation validation and closure report along with detailed reports as per TAT of 90 days.
- Final Briefing and Executive summary

Timelines: Quarterly/As Applicable/As per Bank's Requirement

7.16 Penetration Testing

Scope of Work

The bidder shall conduct penetration testing to validate exploitable vulnerabilities across identified systems, applications and network infrastructure. The testing shall simulate real-world attack scenarios to assess the effectiveness of existing security controls and defence mechanisms.

- The objective of the assessment is to determine the effectiveness of the security of organization's infrastructure and its ability to withstand an intrusion attempt. This may be achieved by conducting both reconnaissance and a comprehensive penetration test. This will provide good insight as to what an attacker can discover about the network and how this information can be used to further leverage attacks.

- The security assessment should use the industry standard penetration test methodologies (like OSSTM) and scanning techniques and will focus on applications. The application tests should cover but not limited to OWASP Top 10 attacks.

- Consultant shall perform application security testing, to identify security vulnerabilities in the Bank's applications that may be exploited by a user to obtain unauthorized access. This will also include identification of any configuration issues that may not have been possible to identify during traditional vulnerability assessment.
- Consultant shall use automated and manual testing techniques to exploit the weaknesses identified in the application logic, in areas like authentication, authorization, information leakage, field variable control, session timeout & logout, cache control, serve side logic, client-side logic, error handling, application administration and encryption.
- The Scope for penetration testing should include but not limited to list of internet facing websites/ applications.
- It is explicit that penetration tester should conduct vulnerabilities assessment consulting with concerned personnel and proper permission of the Bank. Finally, remediation and recommendations must be provided along with all findings.
- The bidder shall also be required to perform penetration testing through a combination of automated and manual techniques and shall validate the exploitability of identified vulnerabilities so that the report submitted to the Bank is relevant, actionable and free from avoidable false positives.

The following areas are to be considered for penetration testing:

Network Security

- Password Security Testing
- Router Security Assessment
- Anti-Virus System Security Assessment and Management Strategy
- Internet User Security

Host Security

- Unix/Linux System Security Assessment
- Windows System Security Assessment
- Web Server Security Assessment
- Other relevant/mapped application Security Assessment

Database Security Assessment

Scope of work for Penetration Testing

- Tests for default passwords

- Tests for DOS vulnerabilities
- Test for directory Traversal
- Test for insecure services such as SNMP
- Check for vulnerabilities based on version of device/server
- Test for SQL, XSS and other web application related vulnerabilities
- Check for weak encryption
- Check for SMTP related vulnerabilities such as open mail relay
- Check for strong authentication scheme
- Test for sample and default applications/pages
- Check for DNS related vulnerabilities such as DNS cache poisoning and snooping
- Test for information disclosure such as internal IP disclosure
- Look for potential backdoors
- Check for older vulnerable version
- Remote code execution
- Weak SSL Certificate and Ciphers
- Missing patches and versions
- This is a minimum indicative list, vendors are encouraged to check for more settings in line with best practices including PCI, OSSTM etc

API Security

- API Security Testing: Authentication and Authorization testing, Input validation and sanitization testing, API endpoint security testing, Data encryption testing (in transit and at rest), Rate limiting and throttling testing
- Configuration Testing for Weak API keys, Insecure API endpoints, Data exposure through APIs, API versioning and deprecation issues
- OWASP API Security Top 10

Deliverables :

- Scope finalization, target confirmation and test plan
- Penetration Testing Report
- Final Consolidated Report
- Post-remediation validation and closure report along with detailed reports.
- Final Briefing and Executive summary

Timelines : Half Yearly/As Applicable/As per Bank's Requirement

7.17 Web and Application Security Assessment

Scope of Work:

The bidder shall perform comprehensive security assessment of internet-facing and internal web applications, APIs and business applications of the Bank. The assessment shall cover OWASP Top 10 risks, authentication weaknesses, session management issues and application security vulnerabilities.

Scope of Work for Web and Application Security Assessment

A. Technical Assessment

• The assessment should cover both business logic and technical risks

• The assessment report should contain a detailed threat list of the application. The threat list should contain the possible risks to the application both from a business and technical aspect

• The tester should attempt to identify and exploit vulnerabilities that include the OWASP Top 10, including but not limited to:

- Input validation
- Cross site scripting
- SQL and XSL injection
- Cookie modification
- Code execution
- Buffer overflow
- URL manipulation
- Authentication bypass
- File upload vulnerabilities
- Secure implementation of features such as forgot password, password policies enforcement, CAPTCHA etc
- Session hijacking
- CSRF
- Privilege escalation

The report should show risk to the business based on any exploits found.

The assessment report should contain a test plan that shows what tests were conducted and its status.

B. Process Assessment

- Authorization and Segregation of Duties Controls
  - Understand how system entitlements are used to enforce segregation of duties or authorized transactions.

- Perform sample testing of user application entitlements to confirm appropriate segregations of duties are enforced by the system (in a test environment).
- Perform sample testing of user application entitlement to ensure access to enter, approve, and/or modify transactions, data, or system configurations is restricted to authorized personnel (in a test environment).
- Populate issue and findings log with the gaps / deviations /issues noted (if any)

- Assessment of Role based Security for Applications under scope
  - Review of user creation/modification/deletion/maintenance procedures for the in-scope applications
  - Review of privileged access rights granted to application, system administrators, service providers and vendors
  - Assess the process for review of user logs for administrator and system users
  - Review ongoing monitoring of effectiveness of implemented procedures and controls
  - Perform sample testing of application entitlement to ensure access to enter, approve, and/or modify transactions, data, or system configurations is restricted to authorized personnel.
- Review of account and password policy including controls such as
  - Users are assigned unique accounts
  - Adequate passwords are maintained e.g. alphanumeric, minimum number of characters. etc
  - Periodic password changes and preventing repeated use of passwords and review of Implementation of password policy at system and application levels.
  - Account lockout policy for disabling user accounts after limited number of unsuccessful login attempts
  - Segregation of duties controls /maker-checker controls through appropriate design and implementation of user roles/ profiles.
- Understand how system entitlements are used to enforce segregation of duties or authorized transactions.
- Perform sample testing of application's entitlements to confirm appropriate segregations of duties are being enforced by the system (in a test environment).
- Understand how unsuccessful access attempts to applications in scope are logged and monitored
- Review the implementation and effectiveness of user access management in applications in the event of leaves.
- Review the segregation of development, production and test environments of applications

C. Others

- Review the audit trail features of the applications in scope, understand how the audit trail reports are reviewed by BANK to detect errors and understand how the reported errors are corrected in a timely manner.
- Review the maintenance and storage of audit trails and logs in order to assess whether the same can be used for forensic study if required by Bank
- Understand the legal and statutory requirements related to using the applications in scope
- Review other related procedures namely backup, change management, Escrow arrangement for source code and risk management processes for the applications in scope.

Deliverables:

- Identified threats for each application.
- Report of findings and recommendations for each application.
- All the reports would be prepared module/functionality-wise keeping the following points in view:
  - The assurance that application functions as intended by Bank's information security policy
  - Identification of gaps/ deviancies/ deficiencies/ vulnerabilities/ risks and detailed observations and its potential impact on the business
  - Industry best practices
  - Specific recommendations for improvement
  - Adequate verifiable audit evidence
- Security and control review report of the applications in scope
- All observations will be thoroughly discussed with team/application owners before finalization of report and the users' views/explanations to be noted for deviations/recommendations. However, this should not influence the independent views/observations of the auditors.
- All the documents and audit evidence, documentary or otherwise with screenshots/gist of discussion with stakeholders
- Action Plan for closure of findings
- Closure reports.

Timelines : Half Yearly/As Applicable/As per Bank's Requirement

7.18 Code Review and Secure Coding Practices

Scope of Work:

The bidder shall carry out code review for applications, modules, components and interfaces identified by the Bank. The scope shall include both business logic review and technical

vulnerability assessment. The code review activity shall cover manual as well as automated analysis of code, architecture understanding, threat profiling, identification of insecure coding practices, credential exposure, sensitive data exposure, input validation weaknesses and weaknesses aligned to OWASP and CWE categories.

The bidder shall also include secure coding advisory and training sessions for developers / application teams, wherever required by the Bank.

- The Bidder shall conduct in-depth understanding of the application architecture
- The Bidder shall prepare a threat profile listing all threats that are applicable to the in-scope application.
- The Bidder shall study the code layout in terms of pages, classes, modules, interfaces and custom protocols etc.
- The Bidder shall conduct manual and automated code review as per criticality of the code.
- The Bidder shall use combination of tools like custom scripts, static code analysers, process, file and registry usage monitors, disassemblers, de-compliers etc.
- The Bidder shall verify the findings reported by the tools and prioritize them based on their criticality and impact.
- The Bidder shall provide training and training for developers on secure coding best practices.

Deliverables:

- Threat model and architecture understanding note
- Application security / code review report
- Secure coding recommendations and remediation advisory
- Developer training / secure coding session(s)
- Validation of implemented fixes and closure report

Timelines : Half Yearly/As Applicable/As per Bank's Requirement

7.19 Mobile Application Security Assessment

The bidder shall perform security assessment of mobile banking and related mobile applications to identify vulnerabilities, insecure APIs, malware risks and mobile platform related threats. The scope shall also include review of Mobile Application Security Assessment mechanisms and security controls.

Identify and verify the mobile application security vulnerabilities against industry global standards such as OWASP, PCI compliance, RBI, etc.

Scope of Work

- Perform assessments to identify vulnerabilities that can be exploited using applications on mobile phones for both registered and anonymous users
- Understand the features, functions in the application
- Create a detailed threat profile and a test plan
- Perform automated and manual tests like HTML Source Code Analysis, SQL Injection, Session Hijacking, LDAP Injection, Authentication Bypass etc.
- Assess adequacy, generation & availability of Reports for accounting, regulatory, statutory, reconciliation, MIS & statistical purpose covering all Mobile banking transactions
- Check Adherence to Operational/Statutory guidelines issued by RBI & other Regulatory bodies w.r.t Mobile Banking Application Perform audit of various functionalities provided in the application like Fund transfer, Transactions & queries, Cheque Book related etc.
- Emergence of fintech partnership for digitization etc.
- Perform verification of the detailed security procedures & processes of the Mobile Banking Solution provider as a part of the existing operational rules & regulations covering transaction, Data & Operational Security setup & establishing the adequacy of the same w.r.t the current Setup.
- Check adequacy Of Operational Security features through Access Control, User Rights, Logging, Data integrity, Accountability, Auditability etc. for the Mobile Application Solution
- Check adequacy of MPIN Management Controls (Generation, Regeneration, Authorization, Verifications etc.) of Mobile Banking & Key Management features.
- Conduct audit of various security features including but not limited to Handset Security features, Transaction level security features, Platform Security & reliability features including Database, Network & transmission Security features, Registration features, Administration Portal features, Call logging, tracking & Dispute Resolution features etc.
- Perform analysis/Verification of Audit Logs /Audit Trails of Transactions, Exception List, Incident management report etc.

Deliverables:

- Threat profile and test plan
- Mobile application security assessment report
- Compliance and control validation report
- Final report with observations and remediation
- Closure validation report

Timelines : Half Yearly/As Applicable/As per Bank's Requirement

7.20 Digital Forensic Services :

Scope of Work

The bidder shall provide digital forensic investigation support for cyber security incidents, compromise assessment and suspicious activities identified by the Bank. The scope shall include evidence collection, log analysis, forensic analysis and reporting support as required and acceptable to the court of law.

a. The bank proposes to engage a Digital Forensic Service provider for investigation, analysis and reporting of cyber security incidents, frauds and policy violations.

b. The service shall support forensic acquisition and analysis of digital evidence from multiple sources, including:

- Servers and endpoints
- Network devices/Solutions and cyber security tools/Solutions / systems
- Databases and storage media
- Email systems and messaging platforms
- Cloud and virtualized environments

c. The service shall ensure forensically sound evidence acquisition, maintaining data integrity through hashing and chain-of-custody documentation.

d. The service shall support live and dead forensics, including memory analysis and volatile data collection, where required.

e. The service shall support timeline reconstruction, root cause analysis and identification of attack vectors and impacted assets.

f. The service shall support malware and artifact analysis, including identification of persistence mechanisms and lateral movement.

g. The service shall provide detailed forensic reports, including executive summary, technical findings, evidence details and remediation recommendations.

h. The service shall support incident response coordination, including working with the bank's Security Operations Centre, Information Security team and other stakeholders.

i. The service shall support legal and regulatory proceedings, including preparation of evidence suitable and acceptable for court or regulatory submission, if required.

j. The service provider shall ensure confidentiality, data privacy and non-disclosure of all information accessed during investigations.

k. The service shall support remote and on-site investigations, as required by the bank.

l. The service shall provide expert assistance during audits, regulatory inspections and law enforcement interactions, if required.

m. The service shall maintain secure storage and controlled access to forensic evidence for the duration specified by the bank.

n. The service shall support post-incident review and lessons-learned sessions to improve the bank's security posture.

Deliverables :

- Incident assessment / triage note
- Evidence acquisition and collection report
- Root cause / technical analysis report
- Final forensic report
- Remedial advisory note and its closure report

Timeline : As and when required/As Applicable/As per Bank's Requirement

7. RESOURCE REQUIREMENT

Sr. No.	Resource Level	Count	Scope of Work	Skill Set
1	Level 2 (Experience between 3 years and 5 years)	7	• VA • PT • Secure Configuration Assessment • Web Application/ API / Mobile Security Assessment • Code Review and Secure Coding Practices • New Business Security • Architecture Review • Tools and Policy Configuration Review	Education Qualification: • B.Tech/B.E in EC or CS or Graduation in Information Security or Cyber Security or MCA Certification: At Least one certification out of • LPT • CCNA • ISO 27001LA/LI • IITL • Security+ • RHCSA • ISO 22301

			• IS Governance and Policy • Cyber Security Resilience	• GCIA • CISM • CISA • CISSP • OSCP • CRTP or certifications as per level 2 or level 3
2	Level 3 (Experience Above 5 years up to 7 years)	4	• IS Governance and Policy • New Business Security • Architecture Review • Cyber Security Tools/Solutions including Network Security Tools/Solutions and Policy Configuration Review • Web Application / API / Mobile Security Assessment • Code Review and Secure Coding Practices • VA • PT • Secure Configuration Assessment	Education Qualification: • B.Tech/B.E in EC or CS or Graduation in Information Security or Cyber Security or MCA Certification: At least one certification out of L2 eligibility is compulsory and at least one of certifications out of • LPT • CCNA • ISO 27001LA/LI • IITL • Security+ • RHCSA • ISO 22301 • GCIA • CISM • CISA • CISSP • OSCP • CRTP
3	Program Director (Experience of above 7 years)	1	Entire Project Management Responsibility	Education Qualification: • B.Tech/B.E in EC or CS or Graduation in Information Security or Cyber Security or MCA

				Certification: At least one certification of L3 is compulsory and at least two certifications out of • LPT • CAN • ISO 27001LA/LI • IITL • Security+ • RHCSA • ISO 22301 • GCIA • CISM • CISA • CISSP • OSCP • CRTP
4	Digital Forensic Lead / Incident Investigation Expert		As per the scope of Work mentioned in this document/RFP	Educational Qualification: • BE/B.Tech/MCA/M.Sc. (IT/Computer Science/Cyber Security) or equivalent. Certifications: At least one certification out of • GCFA • GCFE • GNFA • GREM • CHFI • EnCE • CCE • CFCE

Note:

1. Bidder should submit proof in support of above mentioned criteria while submitting the proposal, the same is to be submitted in the Part I of Technical Bid document. Vendors who do not fulfil the above criteria or who fail to submit proof will be rejected ab initio. Structure of above count of resources activity wise will be discussed with the successful bidder.

2. The Bank has estimated the requirement of 12 On-Site resources for the purpose of commercial evaluation and Total Cost of Ownership (TCO) calculation. However, the bidder shall independently assess the scope, timelines and operational requirements of the engagement and deploy additional resources, if required, at no additional cost to the Bank, for successful execution and timely completion of the services under the RFP. Any deployment of resources beyond the minimum 12 resources shall be solely at the Bidder's discretion and cost, and no additional financial implications shall be borne by the Bank.

8. PROJECT TIMELINES

The successful Bidder is expected to adhere to the timelines as mentioned in the scope of work for each of the services required. The above mentioned milestones will be treated as complete and successful only after obtaining sign off from Bank team at each milestone.

9. CONTRACT RENEWAL

Bank, at its discretion, can opt to renew the contract for additional period of one (1) year depending on Bank's requirement, on and /or mutually agreed terms and conditions with the successful Bidder, subject to satisfactory services rendered during the contract period. Bidder shall provide confirmation of such renewal prior to execution of the renewal agreement. The Bank reserves the right to renew the contract for all or selected service(s)/line item(s), either fully or partially. Accordingly, the requirement, deployment and continuation of resource shall also be renewed only to the extent of the renewal service(s)/line item(s), as determined by the Bank and fresh contract price to be decided proportionately.

10. SLA COMPLIANCE

Bidder should ensure compliance with Service Levels as defined in the RFP.

10.1 SERVICE LEVEL AGREEMENTS (SLA)

Bidder should monitor and maintain the stated service levels to provide quality customer service to the Bank.

Liquidated Damages for delay in Commencement/completion of services solely from the vendor 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.

11. Liquidated Damage

The successful bidder must strictly adhere to the schedules for completing the assignments. Failure to meet these Implementation schedule, unless it is due to reasons entirely attributable to the bank, may constitute a material breach of the successful bidder's performance. In the event that the Bank is forced to cancel an awarded contract (relative to this RFP) due to the successful bidder's inability to meet the established delivery dates, and also the bank may take suitable penal actions as deemed fit.

Penalty: The successful bidder shall agree to the penalties structure in accordance with the following:

The Liquidated Damages (LD) shall be 0.5 % of the respective component, which have been delayed for each week or part thereof for delay until actual delivery or performance. However, the total amount of Liquidated Damages deducted will be pegged at 10% of the total contract value. Once the maximum is reached, the Bank may consider termination of the contract and other penal measure will be taken like forfeiture of EMD, Foreclosure of BG etc.

In this context Bank may exercise both the rights simultaneously and severally. In case the Bank exercises its right to invoke the Bank guarantee and not to terminate the contract, the Bank may instruct to concerned bidder to submit fresh Bank guarantee for the same amount in this regard.

In case delay is attributable to Bank, proper evidence should be produced by Bidder.

12. Land Border Sharing Clause

The Bidder must comply with the requirements contained in O.M. No. 6/18/2019-PPD, dated 23.07.2020 Order (Public Procurement No. 1), Order (Public Procurement No. 2) dated 23.07.2020 and Order (Public Procurement No. 3) dated 24.07.2020. Bidder should submit the undertaking in **Annexure 12** in this regard and also provide copy of registration certificate issued by competent authority wherever applicable.

Para 1 of Order (Public Procurement No. 1) dated 23-7-2020 and other relevant provisions are as follows:

i. Any bidder from a country which shares a land border with India will be eligible to bid in this tender only if the bidder is registered with Competent Authority.
ii. "Bidder" (including the term 'tenderer', 'consultant' or 'service provider' in certain contexts) means any person or firm or company, including any member of a consortium or joint venture (that is an association of several persons, or firms or companies), every artificial juridical person not falling in any of the descriptions of

bidders stated hereinbefore, including any agency branch or office controlled by such persons, participating in a procurement process.

iii. "Bidder from a country which shares a land border with India" for the purpose of this Order means:

a. An entity incorporated, established, or registered in such a country; or
b. A subsidiary of an entity incorporated, established or registered in such a country; or
c. An entity substantially controlled through entities incorporated, established or registered in such a country; or
d. An entity whose beneficial owner is situated in such a country; or
e. An Indian (or other) agent of such an entity; or
f. A natural person who is a citizen of such a country; or
g. A consortium or joint venture where any member of the consortium or joint venture falls under any of the above.

The beneficial owner for the purpose of (iii) above will be as under.

1. In case of a company or limited liability partnership, the beneficial owner is the natural person(s). who, whether acting alone or together, or though one or more judicial person, has a controlling ownership interest or who exercises control through other means.

Explanation

a. "Controlling ownership interests" means ownership of or entitlement to more than twenty five per-cent of shares or capital or profits of the company.
b. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholder's agreements or voting agreements.

2. In case of partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together or through one or more judicial person, has ownership of entitlement to more than fifteen per-cent of capital or profits of the partnership.
3. In case of an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together or through one or more judicial person, has ownership of or entitlement to more than fifteen per-cent of the property or capital or profits of such association or body of individuals.
4. Where no natural person is identified under (1) or (2) or (3) above, the beneficial owner is the relevant natural person(s), who hold the position of senior managing official.
5. In case of trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen per-cent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

iv. An agent is a person employed to do any act for another, or to represent another in dealings with third persons.

13. Monitoring & Audit

Compliance with security best practices may be monitored by periodic computer security audits /Information Security Audits/Statutory and Regulatory audit performed by or on behalf of the Bank. The periodicity of these audits will be decided at the discretion of the Bank. These audits may include, but are not limited to, a review of: access and authorization procedures, backup and recovery procedures, network security controls and program change controls. The successful bidder must provide the Bank access to various monitoring and performance measurement systems. The successful bidder has to remedy all discrepancies observed by the auditors at no additional cost to the bank. The monthly uptime (previous month) report needs to be submitted by the successful bidder before 5th of Every month to Bank at no additional cost to the Bank.

14. Bid Submission

- All responses received after the due date/time be considered late and would be liable to be rejected. GeM portal will not allow lodgement of RFP response after the deadline. It should be clearly noted that the Bank has no obligation to accept or act on any reason for a late submitted response to RFP. The Bank has no liability to any Respondent who lodges a late RFP response for any reason whatsoever, including RFP responses taken to be late only because of another condition while responding.

Instructions to Bidders: e-tendering

E-tendering will be done through GEM portal. Bidders are required to get registered in GEM portal well in time.

Preparation & Submission of Bids

The Bids (Eligibility Cum Technical as well as Commercial) shall have to be prepared and subsequently submitted online only. Bids not submitted "ONLINE" shall be summarily rejected. No other form of submission shall be permitted.

The bidder has to submit their response in GeM portal before the bid end date & time mentioned in the GeM bid document. The physical documents (viz., EMD, Integrity Pact etc.,) should be submitted to the below mentioned officials before the bid end date & time at the Venue specified in the Bid Schedule.

CISO
Information Security Department
4th Floor, Central Bank of India
Plot No -26, Sector-11
CBD Belapur, Navi Mumbai, Maharashtra – 400614
Phone -022-67123586

The Name and address of the Bidder, RFP No. and Due Date of the RFP are to be specifically mentioned on the Top of the envelope containing physical documents.

Do's and Do not's for Bidder

- Registration process for new Bidder's should be completed at the earliest
- Bidder has to prepare for submission of their bid documents online well in advance as the upload process of soft copy of the bid documents may require encryption (large files take longer time to encrypt) and upload of these files to GeM portal depends upon bidder's infrastructure and connectivity.
- To avoid last minute rush for upload bidder is required to start the upload for all the documents required for online submission of bid one week in advance
- Bidder to initiate few documents uploads during the start of the RFP submission and help required for uploading the documents / understanding the system should be taken up with GeM portal support well in advance.
- Bidder should not raise request for offline submission or late submission since only online submission is accepted on GeM portal.
- Part submission of bids by the Bidder's will not be processed and will be rejected.

Terms & Conditions of Online Submission

1. Bank has decided to determine successful bidder through QCBS method through bids submitted on GeM portal. Bidders shall bear the cost of registration on the GeM portal. Bidder is bound to follow rules of GeM portal as per Government guidelines.
2. Bidders at their own responsibility are advised to conduct a mock drill if required.
3. In the event of failure of the internet connectivity (due to any reason whatsoever it may be) Bank will not responsible and Bank will not extend or re-conduct the bid.
4. In order to ward-off such contingent situation, Bidders are advised to make all the necessary arrangements / alternatives such as back –up power supply, connectivity whatever required so that they are able to circumvent such situation and still be able to participate in the Auction successfully.
5. However, the bidders are requested to not to wait till the last moment to quote their bids to avoid any such complex situations.
6. Failure of power at the premises of bidders during the E-Tendering cannot be the cause for not participating in the E-Tendering.
7. On account of this, the time for the E-Tendering cannot be extended and BANK is not responsible for such eventualities.
8. Bank will not have any liability to Bidders for any interruption or delay in access to site of E-Tendering irrespective of the cause.

Tender Schedule (Key Dates)

The Bidders are strictly advised to follow the Dates and Times as indicated in the Time Schedule in the detailed tender Notice for the Tender. All the online activities are time tracked

and the electronic Tendering System enforces time-locks that ensure that no activity or transaction can take place outside the Start and End Dates and time of the stage as defined in the Tender Schedule.

At the sole discretion of the tender Authority, the time schedule of the Tender stages may be extended.

15. Integrity Pact

Each Participating bidder/s shall submit Integrity Pact as per attached **Annexure 6** duly stamped for ₹600. Integrity pact should be submitted by all participating bidders at the time of submission of bid documents or as per satisfaction of the Bank. The Non submission of Integrity Pact as per time schedule prescribed by Bank may be relevant ground of disqualification for participating in Bid process.

Bank has appointed Independent External Monitor (hereinafter referred to as IEM) for this pact, whose name and e-mail ID are as follows:

1. Shri Anant Kumar [Mail ID: anant_in@yahoo.com]
2. Shri Nirmal Anand Joseph Deva [Mail ID: meghanadeva2022@gmail.com]

- For any clarifications/issues, bidders are requested to contact with Bank's personnel in the below mail-id before contacting with IEM.
  smitcsoc@centralbank.bank.in
  smitpurchase@centralbank.bank.in
  cminfosec@centralbank.bank.in
- IEM's task shall be to review – independently and objectively, whether and to what extent the parties comply with the obligations under this pact
- IEM shall not be subjected to instructions by the representatives of the parties and perform his functions neutrally and independently
- Both the parities accept that the IEM has the right to access all the documents relating to the project/procurement, including minutes of meetings.

16. Commercial Offers

Commercial Bids of only technically qualified Bidders shall be opened based on technical proposal.

The Commercial Offer (CO) should be complete in all respect. It should contain only the price information as per Bill of Material

a. The commercial offer should be in compliance with technical configuration / specifications as per Technical Specifications.
b. The price to be quoted for all individual items and it should be unit price in Indian rupees.
c. In case there is a variation between numbers and words, the value mentioned in words would be considered. The Bidder is expected to quote unit price in Indian Rupees (without decimal places) for all components and services on a fixed price basis, as per the

commercial Bid inclusive of all costs except GST. The GST (Goods and Services Taxes) shall be payable as per applicable structure laid down under GST Law. The Bank will not pay any other taxes, cost, or charges. The price would be inclusive of all applicable taxes under the Indian law like customs duty, freight, forwarding, insurance, delivery, etc. including applicable GST, which shall be paid/ reimbursed on actual basis on production of bills with GSTIN. Any increase in GST will be paid in actuals by the Bank or any new tax introduced by the government will also be paid by the Bank. The entire benefits/ advantages, arising out of fall in prices, taxes, duties or any other reason, must be passed on to Bank. The price quoted by the Bidder should not change due to exchange rate fluctuations, inflation, market conditions, and increase in custom duty. The Bank will not pay any out-of-pocket expense. The Selected Bidder will be entirely responsible for license fee, road permits, insurance etc. in connection with the delivery of products at site advised by the Bank including incidental services and commissioning.

d. The price is inclusive of taxes i.e. Goods and Services Tax, which shall be paid as per actuals.
e. Bank will award the contract to the successful Bidder according to the QCBS evaluation determined through GeM Portal.
f. Bank reserves the rights to negotiate with the selected bidder, if required.

17. Evaluation & Acceptance

1. Technical offers will be evaluated on the basis of compliance with eligibility criteria, technical specification, other terms & conditions stipulated in the RFP. Only those bidders who qualify in the technical evaluation would be considered for evaluating the commercial bid. Bank may, at its sole discretion, waive any non-conformity or deviations.

2. Bank reserves the right to reject the bid offer under any of the following circumstances: a) If the bid offer is incomplete and / or not accompanied by all stipulated documents. b) If the bid offer is not in conformity with the terms and conditions stipulated in the RFP.

3. The Bank shall be under no obligation to mandatorily accept the lowest or any other offer received and shall be entitled to reject any or all offers without assigning reasons

18. Evaluation Process

All bids will be evaluated on the basis of technical competence and the price quoted. The Technical Evaluation and the Commercial Evaluation shall have the weightage of 75% and 25% respectively, and this weightage shall be taken into consideration for arriving at the Successful Bidder.

Technical & Commercial Scoring

The Commercial Bid of only technically qualified bids shall be opened.

The score(s) will be calculated for all technically qualified bidders using the formula:
H1 = (Minimum Commercial Quote/Quoted Price) x 25% + (Technical Score/Highest Technical Score) x 75%

Technical will carry 75% weightage and Commercial will carry weightage of 25%. Highest scores so obtained using the above method shall be declared as successful bidders. The bidder with the Highest Combined Score (H1) shall be selected. In case of tie between two or more bidders for the Highest Total Combined Score, then the bidder with Highest Technical Score among such bidders shall be the successful bidder.

Technical offers will be evaluated on the basis of compliance with eligibility criteria, technical specification, other terms & conditions stipulated in the RFP. Only those bidders who qualify in the technical evaluation would be considered for evaluating the Commercial Bid. Bank may, at its sole discretion, waive any non-conformity or deviations. In case, any of the successful bidder is unable to honor in full or part of the contract awarded, Bank shall, at its sole discretion, distribute this shortfall to the other successful bidder(s) equally or in any ratio decided by the Bank.

Bank reserves the right to reject the bid offer under any of the following circumstances:

i). If the bid offer is incomplete and / or not accompanied by all stipulated documents.

ii). If the bid offer is not in conformity with the terms and conditions stipulated in the RFP.

The Bank shall be under no obligation to mandatorily accept the lowest or any other offer

received and shall be entitled to reject any or all offers without assigning reasons.

The proposals will be evaluated in three stages.

Stage 1 – Eligibility Criteria Evaluation

Stage 2 – Technical Bid & Presentation Evaluation

Stage 3 – Commercial Bid Evaluation

All bids shall be evaluated by an Evaluation Committee or sub-committee set up for this purpose by the Bank. The evaluation shall be on the basis of technical competence and the price quoted.

Stage 1-Eligibility Criteria Evaluation

Eligibility criterion for the Bidders to qualify this stage is clearly mentioned in "Eligibility Criteria" section of the RFP.

The Bidders who meet all these criteria would only qualify for the second stage of evaluation. The Bidder would also need to provide supporting documents for eligibility proof. All the credentials of the Bidder necessarily need to be relevant to the Indian market.

Stage 2 Technical Bid and Presentation Evaluation

This evaluation will be done in three broad criteria as under :

Section No	Criteria	Maximum Marks	Min. Qualifying marks	Weightage(%)
1	Technical Criteria	350	245	85
2	Presentation	150	105	15
Total		**500**	**350**	

Bidder has to score minimum 70% marks in each of the above two sections to qualify for the next stage of evaluation.

Example : If bidder X scores : Technical Criteria - 310 and Presentation - 130 in Stage -2 above, in such case the Technical Score calculated will be as below,

Step-1 : As bidder has scored more than 70% for each Section i.e (310/350)*100=88.57%, and (130/150)*100=86.67%, the bidder X qualifies for next step.

Step-2 : The Technical Score of bidder X for each section will be calculated as : (85*310)/350=75.29 and (15*130)/150=13. Accordingly Technical Score of the bidder will be 75.29 + 13= 88.29 out of 100.

Section – 1 – Technical Criteria

SNO	Parameters	Document Required	Max Marks	Marks Scheme
Bidder Experience				
1	The Bidder must have experience and expertise of each of the service as mention below in at least any one **Schedule Commercial Bank with minimum 2000 Branches in India during last 5 years**. The Project must be of **min. 1 year** duration and of min. **Rs. 2 Lacs value per line item.** 1. Vulnerability Assessment 2. Penetration Testing 3. Web & Application Security 4. Code Review and Secure Coding Practices 5. Mobile Application Security Assessment 6. Red Teaming 7. Digital Forensic Services 8. Regulatory Compliance Review 9. Documentation – Policy, Processes, Procedure Creation/Review/ Modification etc.	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience.	180	10 marks for each experience of mentioned service (experience for each mentioned service will be counted max. 2 times)

	(Minimum one experience in above mentioned each service is mandatory)			
2	The Bidder should have experience in below mentioned services in at-least one Scheduled Commercial Bank (SCB) with minimum 2000 Branches in last 5 years in India. The project must be of minimum 1 year and of min. Rs. 2 Lacs per line item. 1. Security and Network Architecture Review 2. Secure Configuration Documentation & Review 3. Cyber Security Tools/Solutions including Network 4. ISO 27001 &/ ISO 22301 Consulting 5. Cyber Security Maturity Assessment 6. SOC Review 7. Cyber Resilience Preparedness	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience.	100	10 marks for each unique service experience

	8. AI Technology Vulnerability Management 9. ISO 42001 Certification Preparation 10. KRI/ KPI Reviews **(Experience in above mentioned services is not mandatory but it is desirable)**			
3	Proprietary tools developed / owned by Bidder	Proof of ownership of the tools	25	5 marks per tool
Team Competency				
4	Experience of the Proposed One Program Director, 4 - L3 resources & 7 - L2 resources in last 3 years from the date of bid submission (For the services mentioned in the RFP)	Details of satisfactory service / implementation by proposed Program Director, L3 and L2 resources to be provided on the letter head of the client. the Program director worked.	45	5 marks for each Experience of Program Director (max. 15 marks) 4 marks for each experience of L3 resources (max. 16 marks) 2 marks for each experience of L2 resources (max. 14 marks) (experience of each

				Program Director /L3/L2 resources for each service will be considered once only)
	Total		**350**	

Section -2 : Presentation by bidder

Presentation by bidder carries marks for various evaluation criteria as mentioned below -

Sr no	Criteria	Max Marks
1	Strategy Articulation & Understanding the project and approach	30
2	Experience and Expertise in Each of the services asked by the Bank	30
3	Team expertise and strength of resources to be deployed	30
4	Proprietary / Owned tools	30
5	Value Addition, Innovation and Maturity Roadmap	30
	Total Marks	**150**

Bidder qualifying with min. 70% will be eligible to participate further for commercial evaluation.

Stage-3 Commercial Evaluation

a) Only those Bidders who have qualified in **Stage 2 above** will be eligible for the further participation in the stage 3 of Commercial Evaluation. The total cost of ownership for the purpose of evaluation shall be calculated over the contract period of 2 years, (total cost of products & services).

b) The score(s) will be calculated for all technically qualified bidders using the formula:

S = (25 x C_minimum/C_quoted) + (75 x T_obtained/T_highest)

(Minimum Commercial Quote/Quoted Price) x 25 + (Technical Score/Highest

Technical Score) x 75. Technical will carry 75% weightage and Commercial will carry weightage of 25%). Bank will award the contract to the successful Bidder whose score "S" is the highest as per the above-mentioned formula. The Bidder shall not add any conditions / deviations in the Commercial Bid. Any such conditions / deviations may make the bid liable for disqualification.

The commercial evaluation would cover Compliance to the Commercial Bid as per in **Annexure 1:** The Bidder is expected to provide their "compliance" against each item stated in the Commercial Bid, this means that the Bidder confirms to the provisioning of the stated product or service and the terms of the RFP and subsequent addendums. Deviations to the Compliance requirements may lead to disqualification.

The Bank may go through a process of technical and/ or commercial evaluation and normalization of the bids to the extent possible and feasible to ensure that Bidders are more or less on the same technical ground. After the normalization process, if the Bank feels that any of the bids need to be normalized and that such normalization has a bearing on the Commercial Bid; the Bank may at its discretion ask all the technically shortlisted Bidders to resubmit the updated technical and Commercial Bids once again for scrutiny. The Bank can repeat this normalization process at every stage of technical submission till the Bank is reasonably satisfied.

The Bidders agree that they have no reservation or objection to the normalization process and all the technically short-listed bidders will, by responding to this detailed document, agree to participate in the normalization process and extend their co-operation to the Bank during this process. The Bidders, by submitting the response to this detailed document, agree to the process and conditions of the normalization process. Any non-compliance to the normalization process may result in disqualification of the concerned Bidder. Bank may call for any clarifications/ additional particulars required, if any, on the technical/Commercial Bids submitted. The Bidder has to submit the clarifications/ additional particulars in writing within the specified date and time. The Bidder's offer may be disqualified, if the clarifications/ additional particulars sought are not submitted within the specified date and time. Bank shall call for presentation(s), product demo/walkthroughs, on the features of the solution offered etc., from the bidders based on the technical bids submitted by them. Bank also reserves the right to conduct reference site visits at the Bidder's client sites. Based upon the final technical scoring, short listing would be made of the eligible bidders for final Commercial Bidding.

Note: Tendering process need not be cancelled merely on the grounds that a single tender was received provided that the single bid received is evaluated to be substantially responsive and deemed fit for award. Bank reserves right to proceed and award the tender to single bidder in

case only one bidder participates in the tender / qualifies in the technical bid evaluation. Bank can negotiate with such single bidder, if required.

Note : As per GeM regulations Bank may scale down over all score of each bidder according to the maximum marks of 100.

19. Payment Terms

Payment will be made as per Regular Cycle or on need basis activity of each service availment instance/cycle as per below milestones and services mentioned:

1. Assessment & Technical Testing Services

(VAPT, Web & Application Security, Mobile Application Security Assessment, Red Teaming, and AI Technology Vulnerability Management)

a. **40% : Upon completion of the initial round of testing and submission of the comprehensive Draft Report / Assessment Findings.**

b. **40% : After the remediation window, upon completion of the Revalidation / Confirmatory Testing round and submission of the Final Report signed off by the Bank.**

c. **20% Retention: After final closure of all bugs or after 90 days of genuine efforts by the successful bidder.**

2. Security Architecture & Configuration Reviews

(Security and Network Architecture Review, Secure Configuration Documentation & Review, Configuration Assessment, and SOC Review)

a. **20% : On completion of data discovery, asset review, and submission of the initial Gap Analysis Report.**

b. **50% : On submission of the Final Architecture Assessment Report containing actionable recommendations.**

c. **30% Milestone Payment: Paid post-implementation support, validating that recommended controls or rules are successfully applied.**

3. Governance, Risk, and Compliance (GRC)

(ISO 27001 / ISO 22301 Consulting, ISO 42001 Certification Prep, Cyber Security Maturity Assessment, KRI/KPI Reviews, Regulatory Compliance Review, Policy/Process Documentation)

a. **30% : On submission and acceptance of the As-Is Assessment and Gap Report.**

b. 40% : On final delivery, approval, and internal deployment of the Drafted/Modified Policies, Processes, and KRI/KPI Frameworks.

c. 30% : Paid after complete formal sign-off.

4. Specialized, Tool-Based & Advisory Services

(Cyber Security Tools/Solutions Assessment, Digital Forensic Services, Cyber Resilience Preparedness, Code Review and Secure Coding Practices)

a. Cyber Security Solutions/Tool Assessments: 50% payment upon final submission of the Product Evaluation and Integration compatibility matrix report. 50% payment upon final revalidation.

b. Code Review and Secure Coding Practices: 100% post completion to Secure Coding Review activity and post-conduct of training, subject to submission of attendance logs, course material, and feedback reports.

c. Forensics : 100% on delivery of the final admissible Forensic Evidence Investigation and closure Report.

d. Cyber Resilience Preparedness : 100% on completion of the activity.

The term of the contract will be 2 years. The Bidder must accept the payment terms proposed by the Bank as proposed in this Section. The financial offer submitted by the Bidder must be in conformity with the payment terms proposed by the Bank. Any deviation from the proposed payment terms would not be accepted.

All / any payments will be made subject to compliance of Service Levels defined in the RFP document. The Bank shall have the right to withhold any payment due to the Bidder, in case of delays or defaults on the part of the Bidder. Such withholding of payment shall not amount to a default on the part of the Bank. If any of the items / activities as mentioned in the price bid is not taken up by the Bank during the course of the assignment, the Bank will not pay the fees quoted by the Bidder in the price bid against such activity / item.

19.1 PROCEDURE FOR CLAIMING PAYMENTS

The Bidder's requests for payment shall be made to the Bank in writing accompanied by Original Invoice detailing the systems, software delivered, installed and accepted by the Bank. The payment after deducting applicable TDS will be released by the Bank. All payments will be made only by electronic transfer of funds either by NEFT or RTGS. The Bidder therefore has to furnish the Bank account number to where the funds have to be transferred for effecting payments. Payments as per the schedule given below will be released only on acceptance of the

order, on signing the agreement / contract by the selected Bidder, on submission of Performance Bank Guarantee and obtaining sign-off for respective payment milestones.

The scope of work is divided in different areas, the payment would be linked to delivery, and acceptance of each area as explained below:

Taxes

1. The consolidated fees and charges required to be paid by the Bank against each of the specified components under this RFP shall be all-inclusive amount with currently (prevailing) applicable taxes. The bidder shall provide the details of the taxes applicable in the invoices raised on the Bank. Accordingly, the Bank shall deduct at source, all applicable taxes including TDS (Tax Deducted at Source) from the payments due/ payments to bidder. The applicable tax shall be paid by the bidder to the concerned authorities.
2. In case of any variation (upward or downward) in Government levies / taxes / etc. up-to the date of providing services , the benefit or burden of the same shall be passed on or adjusted to the Bank. If the service provider makes any conditional or vague offers, without conforming to these guidelines, the Bank will treat the prices quoted as in conformity with these guidelines and proceed accordingly.
3. Goods and Services Taxes (GST) and its Compliance:-
   i. Goods and Services Tax Law in India is a Comprehensive, multi-stage, destination-based tax that will be levied on every value addition. Bidder shall have to follow GST Law as per time being enforced along with certain mandatory feature mentioned hereunder
   ii. TDS (Tax Deducted on Source) is required to deduct as per applicable under GST Law on the payment made or credited to the supplier of taxable goods and services. It would enhance the tax base and would be compliance and self-maintaining tax law based on processes. The statutory compliances contained in the statutes include obtaining registration under the GST law by the existing assesses as well as new assesses, periodic payments of taxes and furnishing various statement return by all the registered taxable person.
   iii. It is mandatory to pass on the benefit due to reduction in rate of tax or from input tax credit (ITR) to the Bank by way of commensurate reduction in the prices under the GST Law.
   iv. If bidder as the case may be, is backlisted in the GST (Goods and Services Tax) portal or rating of a supplier falls below a mandatory level, as decided time to time may be relevant ground of cancellation of Contract.
4. Bank shall deduct tax at source, if any, as per the applicable law of the land time being enforced. The Service provider shall pay any other taxes separately or along with GST if any attributed by the Government Authorities including Municipal and Local bodies or any other authority authorized in this regard.

20. ORDER CANCELLATION

Bank reserves its right to cancel the order in the event of one or more of the following situations:

20.1 Bank reserves the right to cancel the contract placed on the successful bidder and recover expenditure incurred by the Bank under the following circumstances.

20.2 Delay in delivery/deliverable beyond the specified period for delivery/deliverable.

20.3 Any other lapse pertaining to the order from successful bidder / OEM's end.

20.4 If the service provider commits a breach of any of the terms and conditions of the bid, or if the service provider goes into liquidation, voluntarily or otherwise, the Bank reserves the right to cancel the contract.

20.5 Additionally, if an attachment is levied or continues to be levied for a period of seven days upon the effects of the bid, the Bank may take appropriate action.

20.6 If the service provider fails to complete the assignment as per the timelines prescribed in the RFP and any extension allowed, it will be considered a breach of contract, and the Bank reserves its right to cancel the order in the event of delay and forfeit the bid security/performance bank guarantee as liquidated damages for the delay.

20.7 Penalty / Liquidated Damages beyond 10% of the Total Project cost. In addition to the cancellation of purchase order, Bank reserves the right to appropriate the damages by foreclosing the performance bank guarantee.

20.8 After the award of the contract, if the service provider does not perform satisfactorily or delays execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving one month's notice for the same. In this event, the service provider is bound to make good the additional expenditure that the Bank may have to incur in executing the balance contract. This clause is applicable if, for any reason, the contract is cancelled. The Bank reserves the right to recover any dues payable by the service provider from any amount outstanding to the credit of the service provider, including pending bills and/or invoking the bank guarantee under this contract.

20.9 In addition to the cancellation of the purchase order, the Bank reserves the right to appropriate the damages from the Bid Security / Performance Bank Guarantee given by the service provider and/or foreclose the bank guarantee given by the service

provider against the advance payment and may take appropriate action. Further, in case of failure to adhere to the terms and conditions of the RFP in totality, concealment of facts in the tender documents, or failure to fulfil the contractual obligations of the Purchase order, the Bank may debar/blacklist the service provider from participating in future tender processes. The Bank reserves the right to inform IBA/other banks about blacklisting the service provider in case of default in service or delay leading to financial or reputational loss, loss of time of the bank.

21. Project Review

The parties agree to conduct periodic project reviews at key milestones throughout the IT security solution procurement process to assess progress, adherence to scope, schedule, and budget, identify any issues or risks, ensure the quality and functionality of the solution, and implement corrective actions as needed, with summary reports documenting the outcomes and proposed adjustments.

22. Indemnity

The Bidder shall indemnify the Bank, and shall always keep indemnified and hold the Bank, its employees, personnel, officers, directors, harmless from and against any and all losses, liabilities, claims, actions, costs and expenses (including attorney's fees) relating to, resulting directly or indirectly from or in any way arising out of any claim, suit or proceeding brought against the Bank as a result of:

i. Bank's authorized / bona fide use of the Deliverables and/or the Services provided by Bidder under this RFP or any or all terms and conditions stipulated in the SLA (Service level Agreement) or PO and/or
ii. Relating to or resulting directly from infringement of any third party patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided to fulfil the scope of this project.
iii. An act or omission of the Bidder, employees, agents, sub-contractors in the performance of the obligations of the Bidder under this RFP or, any or all terms and conditions stipulated in the SLA(Service level Agreement) or Purchase Order(PO) and/or
iv. Claims made by employees or subcontractors or subcontractors' employees, who are deployed by the Bidder, against the Bank and/or
v. Breach of any of the term of this RFP or breach of any representation or false representation or inaccurate statement or assurance or covenant or warranty of the Bidder under this RFP or; any or all terms and conditions stipulated in the SLA (Service level Agreement) or PO and/or
vi. Any or all Deliverables or Services infringing any patent, trademarks, copyrights or such other Intellectual Property Rights and/or
vii. Breach of confidentiality obligations of the Bidder contained in this RFP or; any or all terms and conditions stipulated in the SLA (Service level Agreement) or PO and/or
viii. Negligence or gross misconduct attributable to the Bidder or its employees, agent or sub-contractors.

The Bidder shall further indemnify the Bank against any loss or damage arising out of claims of infringement of third-party copyright, patents, or other intellectual property issued or registered in India, provided however,

(i) The Bank notifies the Bidder in writing immediately on aware of such claim,

(ii) The Bidder has sole control of defense and all related settlement negotiations,

(iii) The Bank provides the Bidder with the assistance, information and authority reasonably necessary to perform the above, and

(iv) The Bank does not make any statement or comments or representations about the claim without prior written consent of the Bidder, except under due process of law or order of the court. It is clarified that the Bidder shall in no event enter into a settlement, compromise or make any statement (including failure to take appropriate steps) that may be detrimental to the Bank's (and/or its customers, users and Bidders) rights, interest and reputation.

The Bidder shall compensate the Bank for direct financial loss suffered by the Bank, if the Bidder fails to fix bugs, provide the Modifications / Enhancements / Customization as required by the Bank as per the terms and conditions of this RFP and to meet the Service Levels as per satisfaction of the Bank.

Additionally, the Bidder shall indemnify, protect and save the Bank against all claims, losses, costs, damages, expenses, action, suits and other proceedings, suffered by bank due to the following reasons:

i. that the Deliverables and Services delivered or provided under this Agreement infringe a patent, utility model, industrial design, copyright, trade secret, mask work or trademark in any country where the Deliverables and Services are used, sold or received; and/or The Bidder shall indemnify the Bank in case of any mismatch of ITC (Input Tax Credit) in the GSTR 2A, where the Bank does not opt for retention of GST component on supplies.

ii. all claims, losses, costs, damages, expenses, action, suits and other proceedings resulting from infringement of any patent, trade-marks, copyrights etc. or such other statutory infringements under any laws including the Copyright Act,1957 or Information Technology Act, 2000 or any Law, rules, regulation, bylaws, notification time being enforced in respect of all the Hardware, Software and network equipment or other systems supplied by them to the Bank from whatsoever source, provided the Bank notifies the Bidder in writing as soon as practicable when the Bank becomes aware of the claim however:

a. The Bidder has sole control of the defense and all related settlement negotiations.

b. The Bank provides the Bidder with the assistance, information and authority reasonably necessary to perform the above and bidder is aware of the rights to make any statements or comments or representations about the claim by Bank or any regulatory authority. Indemnity would be limited to court or arbitration awarded damages and shall exclude indirect and incidental damages and compensations.

Bidder shall have no obligations with respect to any Infringement Claims to the extent that the Infringement Claim arises or results from:

(i) Bidder's compliance with Bank's specific technical designs or instructions (except where Bidder knew or should have known that such compliance was likely to result in an Infringement Claim and Bidder did not inform Bank of the same);

(ii) Inclusion in a Deliverable of any content or other materials provided by Bank and the infringement relates to or arises from such Bank materials or provided material;

(iii) Modification of a Deliverable after delivery by Bidder to Bank if such modification was not made by or on behalf of the Bidder;

(iv) operation or use of some or all of the Deliverable in combination with products, information, specification, instructions, data, materials not provided by Bidder; or (v) use of the Deliverables for any purposes for which the same have not been designed or developed or other than in accordance with any applicable specifications or documentation provided under the applicable Statement of Work by the Bidder; or

(v) Use of a superseded release of some or all of the Deliverables or Bank's failure to use any modification of the Deliverable furnished under this Agreement including, but not limited to, corrections, fixes, or enhancements made available by the Bidder.

In the event that Bank is enjoined or otherwise prohibited, or is reasonably likely to be enjoined or otherwise prohibited, from using any Deliverable as a result of or in connection with any claim for which Bidder is required to indemnify Bank under this section according to a final decision of the courts or in the view of Bidder, Bidder, may at its own expense and option:

(i) Procure for Bank the right to continue using such Deliverable;

(ii) Modify the Deliverable so that it becomes non-infringing without materially altering its capacity or performance;

(iii) replace the Deliverable with work product that is equal in capacity and performance but is non-infringing; or (iv) If such measures do not achieve the desired result and if the infringement is established by a final decision of the courts or a judicial or extrajudicial settlement, the Bidder shall refund the Bank the fees effectively paid for that Deliverable by the Bank subject to depreciation for the period of Use, on a straight line depreciation over a 5 year period basis.

The foregoing provides for the entire liability of the Bidder and the exclusive remedy of the Bank in matters related to infringement of third party intellectual property rights.

23. Confidentiality & Non-Disclosure

The bidder is bound by this agreement for not disclosing the Banks data and other information. Resources working in the premises of the Bank are liable to follow the rules and regulations of the Bank.

The document contains information confidential and proprietary to the Bank. Additionally, the bidder will be exposed by virtue of the contracted activities to the internal business and operational information of the Bank, affiliates, and/or business partners, disclosure of receipt of this tender or any part of the aforementioned information to parties not directly involved in providing the requested services could result in the disqualification of the bidders, premature termination of the contract, or legal action against the bidder for breach of trust.

No news release, public announcement or any other reference to the order, relating to the contracted work if allotted with the assignment or any program hereunder shall be made without written consent from the Bank.

As the bidder providing support services for multiple Banks, the bidder at all times should take care to build strong safeguards so that there is no mixing together of information/ documents, records and assets is happening by any chance.

The bidder should undertake to maintain confidentiality of the Banks information even after the termination / expiry of the contracts. The successful bidder shall keep all confidential information of the Bank secure and will not disclose or use it for any purpose other than fulfilling this agreement, both during and after the term, as outlines in the Non-disclosure Agreement.

The Non-Disclosure Agreement (NDA) should be entered in to between the Bank and the successful bidder within a period of 21 days from, the date of acceptance of purchase order.

Guarantee on Software License

The bidder shall guarantee that the software supplied under this contract to the Bank is licensed and legally obtained. Software supplied should not have any embedded malicious and virus programs.

24. Force Majeure

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

i. Natural phenomenon, including but not limited to floods, droughts, earthquakes, epidemics,
ii. Situations, including but not limited to war, declared or undeclared, priorities, quarantines, embargoes.
iii. Terrorist attacks, public unrest in work area.

Provided either party shall within seven (7) days from the occurrence of such a cause notify the other in writing of such causes. The Service provider or the Bank shall not be liable for delay in performing his/her obligations resulting from any Force Majeure cause as referred to and / or defined above. The decision regarding whether a particular event as informed by the bidder being a force majeure event, should be regarded as a force majeure event, shall be solely the decision of the bank. Financial reasons or escalation in prices will not fall under "Force Majeure"

In such a case, the time for performance shall be extended by a period(s) not less than the duration of such delay. If the duration of delay continues beyond a period of three months due to force majeure situation, the parties shall hold consultations with each other in an endeavour to find a solution to the problem. However bidder shall be entitled to receive payments for all services actually rendered up to the date of termination of date of agreement. The financial constraints by way of increased cost to perform the obligations shall not be treated as a force majeure situation if the obligations can otherwise be performed.

25. Resolution of Disputes

The Bank and the competent authority of the bidder shall make every effort to resolve amicably, by direct informal negotiation, any disagreement or dispute arising between them under or in connection with the contract. If after thirty days from the commencement of such informal negotiations, the Bank and the Bidder have been unable to resolve amicably a contract dispute, either party may require that the dispute be referred for resolution by formal arbitration.

All questions, disputes or differences arising under and out of, or in connection with the contract shall be referred to a sole arbitrator to be appointed mutually by the parties and in case of failure to appoint a sole arbitrator within 15 days from the raising of dispute the same shall be referred to the Arbitration Tribunal: one Arbitrator to be nominated by the Bank and the other to be nominated by the Bidder and the Presiding Arbitrator shall be appointed by the two Arbitrators appointed by the parties.

The decision of the Arbitration Tribunal shall be final and binding on the parties. The Arbitration and Reconciliation Act 1996 shall apply to the arbitration proceedings and the venue of the arbitration shall be Mumbai. The Language of Arbitration will be English. Notwithstanding the existence of a dispute, and/or the commencement of arbitration proceedings, bidder will continue to perform its contractual obligations and the Bank will continue to pay for all products and services that are accepted by it, provided that all products and services are serving as per the agreed scope between the parties.

If a notice has to be sent to either of the parties following the signing of the contract, it has to be in writing and shall be first transmitted by facsimile transmission, by postage prepaid registered post with acknowledgement due or by a reputed courier service, in the manner as elected by the Party giving such notice. All notices shall be deemed to have been validly given on (i) the business date immediately after the date of transmission with confirmed answer back, if transmitted by facsimile transmission, or (ii) on the date of acknowledgment signed by the receiver or (iii) the business date of receipt, if sent by courier.

This RFP shall be governed and construed in accordance with the laws of India. The courts of Mumbai alone and no other courts shall be entitled to entertain and try any dispute or matter relating to or arising out of this RFP.

26. Independent Contractor

Nothing herein contained will be construed to imply a joint venture, partnership, principal agent relationship or co-employment or joint employment between the Bank and Bidder. Bidder, in furnishing services to the Bank hereunder, is acting only as an independent contractor. Bidder does not undertake by this Agreement or otherwise to perform any obligation of the Bank, whether regulatory or contractual, or to assume any responsibility for the Bank's business or operations. The parties agree that, to the fullest extent permitted by applicable law; Bidder has not, and is not, assuming any duty or obligation that the Bank may owe to its customers or any other person. The bidder shall follow all the rules, regulations statutes and local laws and shall not commit breach of any such applicable laws, regulations etc. In respect of sub-contracts, as applicable – If required by the Bidders, should provide complete details of any subcontractor/s used for the purpose of this engagement. It is clarified that notwithstanding the use of sub-contractors by the Bidder, the Bidder shall be solely responsible for performance of all obligations under the SLA/NDA (Non-Disclosure Agreement) irrespective of the failure or inability of the subcontractor chosen by the Bidder to perform its obligations. The Bidder shall also have the responsibility for payment of all dues and contributions, as applicable, towards statutory benefits including labour laws for its employees and sub-contractors or as the case may be. The bidder should ensure that the due diligence and verification of antecedents of employees/personnel deployed by him for this project are completed and is available for scrutiny by the Bank.

27. Assignment

Bank may assign the Project and the solution and services provided therein by Bidder in whole or as part of a corporate reorganization, consolidation, merger, or sale of substantially all of its assets. The Bank shall have the right to assign such portion of the facilities management services to any of the Contractor/sub-contractor, at its sole option, upon the occurrence of the following: (i) Bidder refuses to perform; (ii) Bidder is unable to perform; (iii) termination of the contract with Bidder for any reason whatsoever;(iv) expiry of the contract. Such right shall be without prejudice to the rights and remedies, which the Bank may have against Bidder. Bidder shall ensure that the said sub-contractors shall agree to provide such services to the Bank

at no less favourable terms than that provided by Bidder and shall include appropriate wordings to this effect in the agreement entered into by Bidder with such sub-contractors. The assignment envisaged in this scenario is only in certain extreme events such as refusal or inability of Bidder to perform or termination/expiry of the contract/project.

28. INSURANCE

The equipment (hardware/software, etc.) supplied under the contract shall be fully insured by the bidder against loss or damage incidental to manufacture or acquisition, transportation, storage, delivery, and installation. The insurance shall be obtained by the Service Provider, naming Central Bank of India as the beneficiary, for an amount equal to 100% of the invoiced value of the goods on an "all risks" basis, covering risks such as damage, theft, fire, or natural disasters. The period of insurance shall remain in effect until the supplied components are accepted by the Bank, and the rights to the property are transferred to the Bank at its premises. In the event of any loss or damage, the bidder shall initiate and pursue the claim until settlement. Additionally, the bidder must promptly make arrangements for the repair and/or replacement of any damaged items, irrespective of the settlement of the claim by the underwriters. Furthermore, the Service Provider shall ensure that the insurance policy remains valid throughout the supply, transportation, and installation period, and any gaps in coverage shall be rectified immediately. The Service Provider shall also provide the Bank with necessary documentation of the insurance policy, claim details, and any associated correspondence with the underwriters.

29. EXECUTION OF CONTRACT, SLA & NDA

The bidder and Bank should execute

1. Contract, which would include all the services and terms and conditions of the services to be extended as detailed herein and as may be prescribed by the Bank and
2. Non-disclosure Agreement.
3. The bidder should execute the contract, SLA and NDA within 21 days from the date of acceptance of the Purchase Order.
4. The term of the contract shall be for a period of 2 years from the date of Go live.
5. In case of any discrepancy among RFP, Purchase Order and SLA, the RFP clauses shall prevail.

30. SUCCESSFUL BIDDER'S LIABILITY

The Bidders aggregate liability in connection with obligations undertaken as a part of the project regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), shall be at actuals and limited to the value of the contract. The

Bidders liability in case of claims against the Bank resulting from wilful misconduct or gross negligence of the Bidder, its employees and subcontractors or from infringement of patents, trademarks, copyrights (if any) or breach of confidentiality obligations shall be unlimited. In no event shall the Bank be liable for any indirect, incidental or consequential damages or liability, under or in connection with or arising out of this tender and subsequent agreement or services provided. The bidder should ensure that the due diligence and verification of antecedents of employees/personnel deployed by him for execution of this contract are completed and is available for scrutiny by the Bank.

Subject to any law to contrary, and to the maximum extent permitted by law neither party shall be liable to other for any remote and indirect loss or damages arising out of this tender and subsequent agreement or services provided."

This limitation shall not apply to third-party claims arising from:

Intellectual Property (IP) Infringement Indemnity: The Bidder's liability for any claim or damages arising from infringement or alleged infringement of third-party intellectual property rights shall not be subject to the above limitation.

Bodily Injury, Death, and Property Damage: The Bidder shall be fully liable for any bodily injury (including death) or damage to real property or tangible property caused by the Bidder's negligence, fraud, or misrepresentation, or that of its employees, representatives, or subcontractors.

31. INFORMATION OWNERSHIP

All information transmitted by successful Bidder belongs to the Bank. The Bidder does not acquire implicit access rights to the information or rights to redistribute the information unless and until written approval sought in this regard. The Bidder understands that civil, criminal, or administrative penalties may apply for failure to protect information appropriately, which is proved to have caused due to reasons solely attributable to bidder. Any information considered sensitive by the bank must be protected by the successful Bidder from unauthorized disclosure, modification or access. The bank's decision will be final if any unauthorized disclosure have encountered. Types of sensitive information that will be found on Bank system's which the Bidder plans to support or have access to include, but are not limited to: Information subject to special statutory protection, legal actions, disciplinary actions, complaints, IT security, pending cases, civil and criminal investigations, etc. The successful Bidder shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the Bidder or existing at any of the Bank location. The Bidder will have to also ensure that all sub-contractors who are involved in providing such security safeguards or part of it shall not publish or disclose in any manner, without the Bank's

prior written consent, the details of any security safeguards designed, developed, or implemented by the Bidder or existing at any Bank location.

32. Inspection, Audit, Review, Monitoring & Visitations

All OEM/Bidder records with respect to any matters / issues covered under the scope of this RFP/project shall be made available to the Bank at any time during normal business hours, to audit, examine, and make excerpts or transcripts of all relevant data. Such records are subject to examination. The cost of such audit will be borne by the Bank. Bidder shall permit audit by internal/external auditors of the Bank or RBI to assess the adequacy of risk management practices adopted in overseeing and managing the outsourced activity/arrangement made by the Bank. Bank shall undertake a periodic review of service provider/BIDDER outsourced process to identify new outsourcing risks as they arise. The BIDDER shall be subject to risk management and security and privacy policies that meet the Bank's standard. In case the BIDDER outsourced to third party, there must be proper Agreement / purchase order with concerned third party. The Bank shall have right to intervene with appropriate measure to meet the Bank's legal and regulatory obligations. Access to books and records/Audit and Inspection would include:-

a. Ensure that the Bank has the ability to access all books, records and information relevant to the outsourced activity available with the bidder. For technology outsourcing, requisite audit trails and logs for administrative activities should be retained and accessible to the Bank based on approved request.
b. Provide the Bank with right to conduct audits on the bidder whether by its internal or external auditors, or by external specialist appointed to act on its behalf and to obtain copies of any audit or review reports and finding made on the service provider in conjunction with the services performed for the bank.
c. Include clause to allow the reserve bank of India or persons authorized by it to access the bank's documents: records of transactions, and other necessary information given to you, stored or processed by the bidder within a reasonable time. This includes information maintained in paper and electronic formats.
d. Recognized the right of the reserve bank to cause an inspection to be made of a service provider of the bank and its books and account by one or more of its officers or employees or other persons. Banks shall at least on an annual basis, review the financial and operational condition of the bidder. Bank shall also periodically commission independent audit and expert assessment on the security and controlled environment of the bidder. Such assessment and reports on the bidder may be performed and prepared by Bank's internal or external auditors, or by agents appointed by the Bank.
e. Any such audit shall be conducted expeditiously, efficiently, and at reasonable business hours after giving due notice to the Bidder which shall not be less than 10 days. The Bank shall not have access to the proprietary data of, or relating to, any other customer of Bidder,

or a third party or Bidder's cost, profit, discount and pricing data. The audit shall not be permitted if it interferes with Bidder's ability to perform the services in accordance with the service levels, unless the Bank relieves Bidder from meeting the applicable service levels. The audit shall not be performed by any competitor of the Bidder. The auditor including regulatory auditor shall sign the confidentiality undertaking with the Bidder before conducting such audit.

Monitoring

Compliance with Information security best practices may be monitored by periodic Information security audits performed by or on behalf of the Bank and by the RBI. The periodicity of these audits will be decided at the discretion of the Bank. These audits may include, but are not limited to, a review of: access and authorization procedures, physical security controls, backup and recovery procedures, network security controls and program change controls. To the extent that the Bank deems it necessary to carry out a program of inspection and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of data, the Service Provider shall afford the Bank's representatives access to the Bidder's facilities, installations, technical resources, operations, documentation, records, databases and personnel. The Bidder must provide the Bank access to various monitoring and performance measurement systems (both manual and automated). The Bank has the right to get the monitoring and performance measurement systems (both manual and automated) audited by prior notice to the Bidder.

Visitations

The Bank shall be entitled to, either by itself or its authorized representative, visit any of the Bidder's premises by prior notice to ensure that data provided by the Bank is not misused.

The Bidder shall cooperate with the authorized representative(s) of the Bank and shall provide all information/ documents\required by the Bank.

33. INFORMATION SECURITY

System should have standard input, communication, processing and output validations and controls. System hardening should be done by bidder. Access controls at DB, OS, and Application levels should be ensured. Bidder should comply with the Information Security Policy of the Bank. The Product offered should comply with regulator's guidelines. The bidder shall disclose security breaches if any to the Bank, without any delay.

The following mandatory security controls must be ensured by the Bidder for proposed Solutions:

a. There should be mechanisms in place to secure the Data from loss, misuse, or disclosure.

b. The platform and solution should encrypt/tokenize data at rest.

c. There should be encryption and integrity protection in place for all internal network traffic that potentially carries sensitive information (including passwords, emails, files, source code, management traffic, etc.)

d. The passwords should be encrypted.

e. The Solution should handle personally identifiable information (PII) as per the statutory guidelines.

f. Testers and developers should be prevented from accessing production systems.

g. The application should have role-based access for customers and third-party users.

h. The system should define groups of leads that are only accessible to certain specified users for marketing purposes.

i. The system should define groups of assets (emails, landing pages, etc.) that can only be accessed by certain specified users.

j. The solution should ensure PII data security.

k. The bidder should comply with various guidelines issued by regulatory / statutory bodies such as Govt of India, RBI, UIDAI, NCIIPC, EASE such as RBI Working group document on "Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds" dated Jan 2011, such as for confidentiality and security and Cyber Security guideline June' 2016, RBI February 2021 Master Circular on Digital Payments Security, RBI circular on "Storage of Payment System Data" dated April 6, 2018, RBI's Master Directions on Outsourcing of Information Technology Services dated 10th April 2023, Digital Personal Data Protection (DPDP) Act 2023 of Government of India etc. with respect to implementation and maintenance of proposed Solutions.

l. Scalability and Availability: The solution's architecture must support high scalability and availability. The vendor should provide a high-level architectural design of the application including this network topology.

34. Intellectual Property Rights

The Bidder claims and represents that it has obtained appropriate rights to provide the Deliverables upon the terms and conditions contained in this RFP. The Bank agrees and acknowledges that same as expressly provided in this RFP, all Intellectual Property Rights in relation to the Hardware, Software and Documentation and any adaptations, translations and derivative works thereof whether protectable as a copyright, trade mark, patent, trade secret design or otherwise, provided by the Bidder during, in connection with or in relation to fulfilling its obligations under this RFP belong to and shall remain a property of the Bidder or its licensor. During the Term of this Project and, if applicable, during the Reverse Transition Period, Bank grants Bidder a right to use at no cost or charge the Hardware and Software licensed to the Bank, solely for the purpose of providing the Services. The Bidder shall be responsible for obtaining all necessary authorizations and consents from third party licensors of Hardware and Software used by Bidder in performing its obligations under this Project. If a third party's claim endangers or disrupts the Bank's use of the Hardware and Software, the Bidder shall at no further expense, charge, fees or costs to the Bank, (i) obtain a license so that the Bank may

continue use of the Software in accordance with the terms of this tender and subsequent Agreement and the license agreement; or (ii) modify the Software without affecting the functionality of the Software in any manner so as to avoid the infringement; or (iii) replace the Software with a compatible, functionally equivalent and non-infringing product. All third party Hardware/software / service/s provided by the bidder in the scope of the RFP will be the responsibility of the bidder if any discrepancy or infringement is encountered. The Bank shall not be held liable for and is absolved of any responsibility or claim/Litigation or penal liability arising out of the use of any third party software or modules supplied by the Bidder as part of this Project.

Bidder's Proprietary Software and Pre-Existing IP:- Bank acknowledges and agrees that this is a professional services agreement and this agreement is not intended to be used for licensing of any Bidder 's proprietary software or tools. If Bidder and Bank mutually agree that the Bidder provides to Bank any proprietary software or tools of Bidder or of a third party, the parties shall negotiate and set forth the applicable terms and conditions in a separate license agreement and the provisions of this Clause shall not apply to any deliverables related to customization or implementation of any such proprietary software or products of Bidder or of a third party. Further, Bank acknowledges that in performing Services under this Agreement Bidder may use Bidder 's proprietary materials including without limitation any software (or any part or component thereof), tools, methodology, processes, ideas, know-how and technology that are or were developed or owned by Bidder prior to or independent of the Services performed hereunder or any improvements, enhancements, modifications or customization made thereto as part of or in the course of performing the Services hereunder, ("Bidder Pre-Existing IP"). Notwithstanding anything to the contrary contained in this Agreement, Bidder shall continue to retain all the ownership, the rights title and interests to all Bidder Pre-Existing IP and nothing contained herein shall be construed as preventing or restricting Bidder from using Bidder Pre-Existing IP in any manner. To the extent that any Bidder Pre-Existing IP or a portion thereof is incorporated or contained in a deliverable under this Agreement, Bidder hereby grants to Banka non-exclusive, perpetual, royalty free, fully paid up, irrevocable license, with the right to sublicense through multiple tiers, to use, copy, install, perform, display, modify and create derivative works of any such Bidder Pre-Existing IP in connection with the deliverables and only as part of the Deliverables in which they are incorporated or embedded. The foregoing license does not authorizes Bank to (a) separate Bidder Pre-Existing IP from the deliverable in which they are incorporated for creating a stand-alone product for marketing to others; (b) independently sell, lease, exchange, mortgage, pledge, license, sub license, assign or in any other way convey, transfer or alienate the Bidder Pre-Existing IP in favour of any person (either for commercial consideration or not (including by way of transmission), and/or (c) except as specifically and to the extent permitted by the Bidder in the relevant Statement of Work, reverse compile or in any other way arrive at or attempt to arrive at the source code of the Bidder Pre-Existing IP.

Residuary Rights. Each Party shall be entitled to use in the normal course of its business and in providing same or similar services or development of similar deliverables for its other clients,

the general knowledge and experience gained and retained in the unaided human memory of its personnel in the performance of this Agreement and Statement of Work(s) hereunder. For the purposes of clarity the Bidder shall be free to provide any services or design any deliverable(s) that perform functions same or similar to the deliverables being provided hereunder for the Client, for any other customer of the Bidder (including without limitation any affiliate, competitor or potential competitor of the Bank. Nothing contained in this Clause shall relieve either party of its confidentiality obligations with respect to the proprietary and confidential information or material of the other party

35. VISITORIAL RIGHTS

The Bank and its authorized representatives reserve the right to visit any of the Bidder's premises without prior notice to ensure that data provided by the Bank is not misused. The bidder shall cooperate with the authorized representative/s of the Bank and shall provide all information/ documents required by the Bank. Non-cooperation by the bidder in this regard will be treated as breach of agreement/Purchase Order and will follow the consequences accordingly.

36. TERMINATION

Central Bank of India reserves the right to cancel the work/purchase order or terminate the Service Level Agreement (SLA) by providing 90 (ninety) days' prior written notice and recovering any damages, costs, and expenses incurred by the Bank under the following circumstances:

GROUNDS OF TERMINATION

i. **Breach of Terms**: If the bidder commits a breach of any of the terms and conditions of the Request for Proposal (RFP) or the Service Level Agreement (SLA) to be executed between the Bank and the SP.

ii. **Insolvency**: If the bidder goes into liquidation, voluntarily or otherwise.

iii. **Violation of Laws**: If the bidder violates any laws, rules, regulations, byelaws, guidelines, or notifications.

iv. **Legal Attachment**: If an attachment is levied or continues to be levied for a period of seven days on the effects of the bid.

v. **Failure to Meet Timelines**: If the bidder fails to complete the assignment as per the timelines prescribed in the Work Order/SLA, including any extensions granted.

vi. **Excess Liquidated Damages**: If the deductions due to liquidated damages exceed 10% of the total work order.

vii. **Failure to Deliver Resources**: If the bidder fails to deliver the required resources as stipulated in the delivery schedule, the Bank reserves the right to procure similar resources from alternative sources at the risk, cost, and responsibility of the bidder.

viii. **Non-Performance**: If after the award of the contract, the bidder fails to perform satisfactorily or causes delays, the Bank reserves the right to have the remaining contract executed by another party of its choice. The bidder must cover any additional expenditure incurred by the Bank in this regard.

ix. **Outstanding Dues**: The Bank reserves the right to recover any dues payable by the bidder from any amount outstanding, including pending bills and/or invoking the Performance Bank Guarantee under this contract.

TYPES OF TERMINATION

i. **Termination for Insolvency**: The Bank may terminate the contract if the bidder becomes bankrupt or insolvent, with termination being without compensation to the bidder. However, this does not affect any accrued rights or remedies of the Bank.

ii. **Termination for Default**: The Bank may terminate the contract in whole or in part, by providing written notice in case of a default by the bidder.

iii. **Termination for Convenience**: The Bank may terminate the contract at its convenience, in whole or in part, with written notice.

EFFECT OF TERMINATION

i. **Transition and Business Continuity**: Upon termination, the Bank is entitled to impose necessary obligations and conditions to ensure smooth transition and business continuity of the services. The bidder must take all steps to minimize loss caused by termination and allow the next successor bidder to take over the obligations.

ii. **Post-Termination Assistance**: If the contract expires or is not extended, the bidder must assist the successor or the Bank's representative with the transition.

This may include providing training or any other necessary support even beyond the contract's termination period.

RIGHT TO TRANSFER IT OUTSOURCING ARRANGEMENTS

In the event of termination, the Bank reserves the right to orderly transfer the proposed IT outsourcing arrangement to another service provider, if necessary or desirable, to ensure minimal disruption of services. This transfer shall be managed in an efficient manner, with the bidder cooperating fully with the Bank to facilitate this process, including transferring knowledge, data, and providing assistance as required.

The termination shall not affect any accrued rights or liabilities of either party and will not affect the provisions that are intended to continue after termination.

37. Exit option and Contract Re-Negotiation

i. The Bank reserves the right to cancel the contract and debar bidder from participating in future procurement processes if one or more of the following conditions occur:

- Failure of bidder to accept the contract or purchase order and to furnish the Performance Guarantee within 21 days of the acceptance of the purchase contract.
- Delay in offering the required deliverables or services.
- Delay in commissioning the project beyond the specified period.
- Delay in completing commissioning, implementation, and acceptance tests/checks beyond the specified periods.
- Serious discrepancies in the project noticed during the testing phase.
- Serious discrepancies in the functionality to be provided or the performance levels agreed upon, which negatively affect the functioning of the Bank.
- Serious discrepancies in the completion of the project.

ii. In addition to cancelling the purchase contract, the Bank reserves the right to appropriate damages by encashing the Bid Security or Performance Guarantee provided by bidder.

iii.The Bank reserves the right to purchase the equipment from third-party suppliers if such equipment is available at a lower price, and if bidder's offer does not match that lower price. However, this will be done only if:

a. The equipment is available at more favourable terms in the industry.

b. The equipment procured from third parties is functionally similar to the original equipment, ensuring that bidder can maintain it.

In addition to the cancellation of purchase contract, Bank reserves the right to appropriate the damages through encashment of Bid Security / Performance Guarantee given by the Bidder.

Notwithstanding the existence of a dispute, and/or the commencement of arbitration proceedings, the Bidder will be expected to continue to provide services to the Bank as per the contract. Bank will continue to pay for all products and services that are accepted by it provided that all products and services as serving as per the agreed scope between the parties. The Bank shall have the sole and absolute discretion to decide whether proper reverse transition mechanism over a period of 6 to 12 months, has been complied with. In the event of the conflict not being resolved, the conflict will be resolved through Arbitration. The Bank and the Bidder shall together prepare the Reverse Transition Plan. However, The Bank shall have the sole decision to ascertain whether such Plan has been complied with. Reverse Transition mechanism would typically include service and tasks that are required to be performed / rendered by the Bidder to The Bank or its designee to ensure smooth handover and transitioning of Bank's deliverables, maintenance and services.

Notwithstanding anything contained in this RFP, Bank reserve the right to cancel the contract by giving 90 days notice period without assigning any reason as per its convenience.

38. Privacy & Security Safeguards

i. The Bidder shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the Bidder or existing at any Bank location. The Bidder will have to develop procedures and implementation plans to ensure that IT resources leaving the control of the assigned user (such as being reassigned, removed for repair, replaced, or upgraded) are cleared of all Bank data and sensitive application software. The Bidder will have to also ensure that all subcontractors who are involved in providing such security safeguards or part of it shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the Bidder or existing at any Bank location.
ii. The Bidder hereby agrees and confirms that they will disclose, forthwith, instances of security breaches.
iii. The Bidder hereby agrees that they will preserve the documents.

39. Governing Law and Jurisdiction

The provisions of this RFP and subsequent Agreement shall be governed by the laws of India. The disputes, if any, arising out of this RFP/Agreement shall be submitted to the jurisdiction of the courts/tribunals in Mumbai.

Statutory and Regulatory Requirements

The solution must comply with all applicable requirements defined by any regulatory, statutory or legal body which shall include but not be limited to RBI or other Regulatory Authority, judicial courts in India and as of the date of execution of Agreement. This requirement shall

supersede the responses provided by the Bidder in the technical response. During the period of warranty / AMC, Bidder / Bidder should comply with all requirements including any or all reports without any additional cost, defined by any regulatory authority time to time and which fall under the scope of this RFP / Agreement. All mandatory requirements by regulatory / statutory bodies will be provided by the bidder under change management at no extra cost to the bank during the tenure of the contract.

40. Compliance with Laws

1. Compliance with all applicable laws: Successful bidder shall undertake to observe, adhere to, abide by, comply with the Bank about all laws in force or as are or as made applicable
2. in future, pertaining to or applicable to them, their business, their employees or their obligations towards them and all purposes of this scope of work.
3. Compliance in obtaining approvals/permissions/licenses: Bidder shall promptly and timely obtain all such consents, permissions, approvals, licenses, etc., as may be necessary or required for any of the purposes of this project or for the conduct of their own business under any applicable Law, Government Regulation/Guidelines and shall keep the same valid and in force during the term of the project.
4. The Annual Technical Support under the RFP should comply with all the Regulatory/ Compliance guideline of the Banks/ Regulatory authority in India. Bank has right to change the compliance/ guideline at any point of time and the service provider has to comply with the guidelines. Bank has right to audit by regulatory authority or any agency appointed by the Bank, as a part of Vendor Audit. The service should comply with Bank IT/ Information Security (IS) / BCP Policy. It will be mandatory to protect the data privacy, as per Indian Data Privacy Law. Service provider should comply with all such laws in existence currently or introduced in future by the Govt. agencies or any other regulatory body.

41. Regulatory compliance

a. The bidder must ensure that the proposed Solutions, platform and implementation, architecture should adheres to guidelines issued by regulatory / statutory bodies such as Govt of India, RBI, UIDAI, SEBI, IRDAI, NCIIPC, TRAI, IFSCA including but not limited to RBI Working group document on "Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds" dated Jan 2011, for confidentiality and security and Cyber Security guideline June' 2016, RBI February 2021 Master Circular on Digital Payments Security, RBI circular on "Storage of Payment System Data" dated April 6, 2018, RBI's Master Directions on Outsourcing of Information Technology Services dated 10th April 2023, Digital Personal Data Protection (DPDP) Act 2023 of Government of India, ISO 27001, ISO 22301, ISO 27701.

b. Any implementation/changes//customizations/enhancements forming part of existing and future statutory and regulatory requirements under the directives of Government of India (GOI), Reserve Bank of India (RBI), MeITY, Cert-In, NCIIPC, UIDAI,

IFSCA etc. should be carried out by the Bidder during the entire contract period without any cost to the Bank.

c. Bidder shall undertake to observe, adhere to, abide by, comply with the Bank about all laws in force or as are or as made applicable in future, pertaining to or applicable to them, their business, their employees or their obligations towards them and all purposes of this scope of work.

d. Bidder shall permit audit by internal/external auditors of the Bank or RBI to assess the adequacy of risk management practices adopted in overseeing and managing the outsourced activity/arrangement made by the Bank. Bank shall undertake a periodic review of service provider/Bidder outsourced process to identify new outsourcing risks as they arise.

e. The warranty and AMC of the proposed software shall include all version upgrade, patches/fixes, upgrades, compliance of mandates (legal guidelines of GOI as per Gazette of India, regulatory authorities, RBI, etc.) and maintenance support, troubleshooting, performance fine tuning, problem resolution for the OS, database, middleware and the application software for total solution provided by the Bidder.

f. Bidder should carry out the backup, storage and restoration as part of the scope of the RFP document to enable the Bank to achieve regulatory compliance and as per Bank's ISMS & BCMS Policies, RBI, NCIIPC (National Critical Information Infrastructure Protection Centre), NCRF guidelines.

42. Violation of Terms

The Bank clarifies that the bank shall be entitled to an injunction, restraining order, right for recovery, specific performance or such other equitable relief as a court of competent jurisdiction may deem necessary or appropriate to restrain the bidder from committing any violation or enforce the performance of the covenants, obligations and representations contained under the RFP/Agreement. These injunctive remedies are cumulative and are in addition to any other rights and remedies the bank may have at law or in equity, including without limitation a right for recovery of any amounts and related costs and a right for damages.

43. Data localization

The service provider shall ensure that all data, as applicable to the concerned bank, is stored exclusively within India, in full compliance with the extant regulatory requirements set forth by the relevant authorities. The service provider shall not store or process any data outside of India without prior written consent from the bank and approval from regulatory bodies.

44. Corrupt & Fraudulent Practices

As per Central Vigilance Commission (CVC) directives, it is required that Bidders / Suppliers / Contractors observe the highest standard of ethics during the procurement and execution of such contracts in pursuance of this policy:

"Corrupt Practice" means the offering, giving, receiving or soliciting of anything of values to influence the action of an official in the procurement process or in contract execution AND

"Fraudulent Practice" means a misrepresentation of facts in order to influence a procurement process or the execution of contract to the detriment of The Bank and includes collusive practice among Bidders (prior to or after offer submission) designed to establish offer prices at artificial non-competitive levels and to deprive The Bank of the benefits of free and open competition.

The Bank reserves the right to reject a proposal for award if it determines that the Bidder recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question. The Bank reserves the right to declare a firm ineligible, either indefinitely or for a stated period of time, to be awarded a contract if at any time it determines that the firm has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

45. PUBLICITY

Any publicity by either party in which the name of the other party is to be used should be done only with the explicit written permission of such other party.

46. APPLICABILITY OF PREFERENCE TO MAKE IN INDIA, ORDER 2017 (PPP-MII ORDER)

Government guidelines on Public Procurement (Preference to Make in India), Order 2017 (PPP-MII Order) and subsequent revision vide Order No. 45021/2/2017-PP(BE-II) dated 16.09.2020 and any revision thereto will be applicable for this RFP.

47. COMPLIANCE TO RBI MASTER DIRECTION ON OUTSOURCING OF IT SERVICES (RESERVE BANK OF INDIA (COMMERCIAL BANKS – MANAGING RISKS IN OUTSOURCING) DIRECTIONS, 2025

a). Regular Monitoring And Assessment Of The Service Provider By Bank

The Bank shall have the right to conduct regular monitoring and assessment including periodic audits, reviews, and security checks of Successful bidder 's performance, security practices,

and compliance with the terms of this agreement. The Successful bidder shall cooperate with the Bank during these assessments and take corrective actions as required.

Type of material adverse events and the incidents required to be reported to Bank by the service provider

i. The Successful bidder shall promptly report any material adverse events, including (but not limited to)
   a. Data breaches
   b. Denial of service attacks
   c. Service unavailability
   d. Security vulnerabilities
   e. Unauthorized access
   f. System failures
   g. Any other incidents that may impact Bank's operations or data integrity.
ii. Such incidents shall be reported to the Bank immediately upon identification, enabling the Bank to take prompt risk mitigation measures and ensure compliance with statutory and regulatory guidelines.
iii. The Successful bidder shall provide all relevant details and updates regarding the incident, including the nature, scope, impact, and corrective actions taken, in accordance with the Bank's incident reporting procedures.

b). Storage of data only in India as per extant regulatory requirements

The Prospective Successful bidder (Service Provider) shall ensure that Bank's data processed or handled under this agreement is stored exclusively within India, in compliance with the extant regulatory requirements.

c). Service provider to provide details of data (related to Bank and its customers) captured, processed and stored

The Successful bidder shall provide the Bank with details of all data related to the Bank and its customers that it captures, processes, and stores, upon receiving an approved request.

d). Controls for maintaining confidentiality of data of Bank and its customers', and incorporating service provider's liability to Bank in the event of security breach and leakage of such information

With related to confidentiality of data,

a) The Successful bidder shall treat all data of the Bank and its customers as confidential and shall not disclose or allow access to such data to any unauthorized third party without the prior written consent of the Bank.
b) The Successful bidder shall implement all necessary measures to protect the confidentiality and integrity of the data throughout the term of this Agreement and thereafter.
c) The Successful bidder shall implement and maintain industry-standards controls to safeguard Bank related data.

e). Types of data/information that the service provider (successful bidder) is permitted to share with Bank's customer and/or any other party

The Successful bidder shall define and ensure the types of data/information that is shared with the Bank's customers and/or any other parties:

i. Is shared with explicit written consent or authorization from the Bank.
ii. Is required by law or regulation, including legal processes such as subpoenas.
iii. Is shared with approved third-party successful bidder or sub-processors.

f). Contingency plan(s) to ensure business continuity and testing requirements

i. The Successful bidder shall have a documented Business Continuity Plan in place, which outlines the strategies for maintaining service availability in the event of an unexpected incident. The Business Continuity Plan should include, but not limited to:
   a. Detailed procedures for mitigating and recovering from various business disruptions.
   b. Identification of key personnel, roles, and responsibilities in a crisis.
   c. Communication plans to inform both Successful bidder and Bank, of significant disruptions and progress towards recovery.
ii. The Successful bidder shall maintain a Disaster Recovery Plan to restore critical services and infrastructure in the event of a disaster, including:
   a. Specific recovery objectives, such as Recovery Time Objective (RTO) and Recovery Point Objective (RPO), to be met for each service.
   b. Procedures for data backup, storage, and retrieval.
   c. Clear steps to restore services to full functionality, including resource allocation and escalation procedures.

g). Right to seek information from the service provider about the third parties (in the supply chain) engaged by the former

The Bank reserves the right to seek information from the Successful bidder about its third parties or sub-contractors engaged in the supply chain or any sub-contracted work.

h). Making the service provider contractually liable for the performance and risk management practices of its sub-contractors

The Successful bidder shall be contractually liable for the performance and risk management practices of its sub-contractors. The Successful bidder will remain fully responsible for ensuring that its sub-contractors adhere to the same performance standards, security protocols, and risk management practices as outlined in the agreement with the Bank. The Successful bidder should be obligated to manage and mitigate any risks arising from its sub-contractors' actions or failures, and to promptly address any issues related to sub-contractor performance that could impact the quality of service or compliance with the agreement.

i). Need of prior approval/consent of the Bank for use of sub-contractors by the service provider for all or part of an outsourced activity

The Successful bidder shall obtain the Bank's prior written consent before sub-contracting or outsourcing all or part of activities covered under this agreement.

j). Termination rights of the Bank, including the ability to orderly transfer the proposed IT-outsourcing arrangement to another service provider, if necessary or desirable

In the event of termination, the Bank shall have the right to transition of the IT outsourcing arrangement to another sub-successful bidder , either in whole or in part, at its discretion. The Successful bidder agrees to fully cooperate with the Bank to ensure an orderly and seamless transfer of services, including the transfer of data, systems, and knowledge, and to provide necessary support to the new Service Provider. The Successful bidder shall also assist in mitigating any risks associated with the transition and shall ensure that all customer data and confidential information is securely handled during the transition process.

k). Obligation of the service provider to co-operate with the relevant authorities in case of insolvency/resolution of the Bank

If the Bank becomes subject to insolvency proceedings, financial restructuring, or resolution by relevant authorities (e.g., governmental bodies, regulatory agencies, or liquidators), the Successful bidder shall co-operate fully with the relevant authorities in accordance with applicable laws and regulations.

The bidder agrees to provide all necessary information, documentation, and assistance as requested by the relevant authorities, including but not limited to access to data, records, systems, and personnel, to ensure a smooth transition or orderly resolution process.

In the event of insolvency or resolution of the Bank, the bidder shall continue to perform its obligations under this Agreement unless otherwise directed by the relevant authorities or instructed by Bank.

The bidder shall notify the Bank promptly upon learning of any insolvency, liquidation, or resolution proceedings involving the Bank, and shall comply with any directions provided by the relevant authorities.

l). Provision to consider skilled resources of service provider who will provide core services as "essential personnel" so that a limited number of staff with back-up arrangements necessary to operate critical functions can work on-site during exigencies (including pandemic situations)

a. The Successful bidder shall designate and maintain a pool of skilled resources who will be considered "essential personnel" for the delivery of core services under this agreement.
b. These personnel will be responsible for ensuring the continuity of critical functions, particularly during exigent circumstances such as emergencies, natural disasters, or pandemics.
c. In the event of such situations, the Successful bidder shall implement necessary backup arrangements to ensure that a limited but enough essential personnel are available to work on-site to support critical operations.
d. The Successful bidder shall make reasonable efforts to ensure the safety and well-being of these personnel while maintaining the uninterrupted delivery of critical services.

e. The Successful bidder shall notify the Bank promptly of any significant changes to the availability or capacity of essential personnel, as well as any potential impact on service delivery.

m). Suitable back-to-back arrangements between service providers and the OEMs

The Successful bidder shall ensure that suitable back-to-back arrangements are in place with Original Equipment Manufacturers (OEMs) to guarantee the provision of required products, services, and support. These arrangements must align with the terms and service levels defined in this agreement, ensuring that the Successful bidder can meet its obligations to the Bank and address any issues related to the OEM products or services in a timely and efficient manner. The Successful bidder is responsible for ensuring that the OEM's support and performance meet the agreed-upon standards, and for providing any necessary escalations or resolutions in the event of failure by the OEM to meet such standards.

48. Sustainable Sourcing

The Supplier shall adhere to Sustainable Sourcing practices including but not limited to the use of environment friendly materials, ethical labour practices and compliance with relevant local and international regulations. The Supplier shall provide documentation or certifications demonstrating their commitment to Sustainable Sourcing upon request. Failure to comply with these requirements may result in contract termination.

49. Entire Agreement; Amendments

This RFP sets forth the entire agreement between the Bank and the Successful bidder and supersedes any other prior proposals, agreements and representations between them related to its subject matter, whether written or oral. No modifications or amendments to this Agreement shall be binding upon the parties unless made in writing, duly executed by authorized officials of both parties.

50. Adherence to Cyber Security Policy

Bidder is responsible for complying with the security standards or desired security aspects of all the ICT resources in line with regulatory guidelines from time to time as well as Bank's IT/Information Security / Cyber Security Policy guidelines. Such guidelines will be shared with bidder. Bidder should ensure Data Security and protection of facilities/application managed by them.

The deputed persons should be aware about Bank's IT/IS/Cyber security policy guidelines and have to maintain the utmost secrecy & confidentiality of the bank's data including process performed. At any time, if it comes to the notice of the bank that data has been compromised/disclosed/misused/misappropriated then bank would take suitable action as deemed fit and selected bidder would be required to compensate the bank to the fullest extent of loss incurred by the Bank.

Bidder has to agree and provide undertaking not to disclose any Bank information and will maintain confidentiality of Bank information as per policy of the Bank and will sign "Non-Disclosure Agreement" document provided by Bank.

The Service provider Shall put in place necessary controls within its organization for maintaining confidentiality of the Bank's and its customers data.

51. Survival and Severability

Any provision or covenant of the RFP, which expressly, or by its nature, imposes obligations on successful bidder shall so survive beyond the expiration, or termination of this Agreement The invalidity of one or more provisions contained in this Agreement shall not affect the remaining portions of this Agreement or any part thereof; and in the event that one or more provisions shall be declared void or unenforceable by any court of competent jurisdiction, this Agreement shall be construed as if any such provision had not been inserted herein.

Bidding Document

The bidder is expected to examine all instructions, forms, terms and conditions and technical specifications in the Bidding Document. Submission of a bid not responsive to the Bidding Document in every respect will be at the bidder's risk and may result in the rejection of its bid without any further reference to the bidder.

52. Amendments to Bidding Documents

The Bank reserves the right to change/modify the dates/terms & conditions without assigning any reasons, mentioned in this RFP document as per its requirement, which will be communicated to the Bidders through Bank's Website. The amendments / clarifications to the tender, if any, will be posted on the Bank website (www.centralbankofindia.bank.in) / GEM Portal. It may be noted that notice regarding corrigenda, addendums, amendments, time-extensions, clarifications, response to bidders' queries etc., if any to RFP, will not be published through any advertisement in newspapers or any other media. Prospective bidders shall regularly visit Bank's website for any changes / development in relation to this RFP. The amendments / clarifications to the tender, if any, will be posted on the Bank website.

53. Period of Validity

Bids shall remain valid for 120 days from the last date of bid submission. A bid valid for shorter period shall be rejected by the bank as non-responsive.

54. Ownership, Grant and Delivery

The Bidder shall procure and provide a non-exclusive, non-transferable, perpetual license to the Bank for all the software to be provided as a part of this project.

The Bank reserves the right to use the excess capacity of the hardware, licenses and other infrastructure supplied by the Bidder for any internal use of the Bank or its affiliates, subsidiaries or regional rural Bank at no additional cost other than the prices mentioned in the commercial bid. The Bidder agrees that they do not have any reservations on such use and will not have any claim whatsoever against such use of the hardware, licenses and infrastructure.

Further, the Bidder also agrees that such use will not infringe or violate any license or other requirements as per applicable intellectual property right.

55. Last Date and Time for Submission of Bids

Bids must be submitted not later than the specified date and time as specified in the Bid Document. Bank reserves the right to extend the date & time without mentioning any reason.

56. Authorized Signatory

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

57. Late Bids

Any bid received after the deadline for submission of bids will be rejected and/or returned unopened to the Bidder, if so desired by him.

58. Modifications and/or Withdrawal of Bids

a. Bids once submitted will be treated as final and no further correspondence will be entertained on this.
b. No bid will be modified after the deadline for submission of bids.
c. No bidder shall be allowed to withdraw the bid, if the bidder happens to be a successful bidder.

Clarification of Bids

To assist in the examination, evaluation and comparison of bids the bank may, at its discretion, ask the bidder for clarification and response, which shall be in writing and without change in the price, shall be sought, offered or permitted.

Bank's Right to Accept or Reject Any or All Bids

The bank reserves the right to accept or reject any bid and annul the bidding process and reject all bids at any time prior to award of contract, without thereby incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidder or bidders of the ground for the bank's action.

59. WAIVER

No waiver of any provision of this Agreement or any of the rights or obligations hereunder shall be effective unless in writing and executed by both parties. A waiver of any breach of any provision of this Agreement shall not be construed as a waiver of any subsequent breach of the same or any other provision. The failure of either party to enforce any provision of this Agreement shall not be deemed a waiver of that provision or of the right of that party thereafter to enforce the same. Any waiver, consent, or approval under this Agreement shall be effective only if it is in writing and signed by the party giving such waiver, consent, or approval.

60.Digital Personal Data Protection Compliance

The Bidder/Vendor shall, always, comply with the provisions of the Digital Personal Data Protection Act, 2023 ("DPDP Act") and the Digital Personal Data Protection Rules, 2025 / Notifications / Guidelines and further rules made thereunder.

The Bidder/Vendor shall implement appropriate technical and organizational measures to ensure lawful processing, secure handling, confidentiality, integrity, availability, and protection of personal data obtained, accessed, shared, or processed in connection with this RFP and the resultant contract.

Further, the Bidder/Vendor shall take due care while collecting and dealing with sensitive personal data or information of Bank and its customer. Any processing of Personal Data by the Service Providers in the performance of the Agreement under this RFP shall follow the above Act/Rules. The Service Provider shall also ensure that any sub-contractor (if allowed) engaged by it shall act in compliance with the above Act, to the extent applicable.

The Bidder/Vendor shall act only on documented instructions of the Bank and shall not process personal data for any purpose other than the performance of the obligations under this RFP.

Any data breach, unauthorised access, misuse, loss, or disclosure of personal data must be reported to the Authority/Bank in writing within [24 hours] of occurrence, along with an incident report and remedial action plan.
The Bidder/Vendor shall indemnify and hold harmless the Bank against any loss, liability, penalty, claim, cost, or damages arising out of non-compliance with the DPDP Act and Rules."

61.Labour Law Adherence and Compliance with Court Directions

The Bidder/Vendor shall ensure full compliance with all applicable labour laws, employment laws, industrial relations regulations, social security legislation, and any orders/directions

issued by competent Labour Courts/Industrial Tribunals/Authorities / RBI and any other Regulatory/ Statutory body in India.

The Bidder/Vendor shall be solely responsible for payment of salaries, wages, statutory contributions, benefits, and all dues to its employees, subcontractors, labour, and statutory personnel deployed for execution of work under this RFP.

No employer-employee relationship shall be deemed to exist between the Bank and the personnel engaged by the Bidder/Vendor.

In case of any claim, demand, dispute, or litigation arising due to non-compliance by the Bidder/Vendor, the same shall be solely borne and resolved by the Bidder/Vendor without any liability upon the Bank.
The Bidder/Vendor shall indemnify the Bank against any losses, costs, or legal liabilities on account of any violation or non-compliance of applicable laws including any liabilities, costs or expenses arising in connection with any proceedings in respect thereof."

62. Change in Location/ Merger/Amalgamation

Bank reserves the right to change the location of services to be provided by the Service Provider by serving prior notice of …. days without assigning any reason and without altering any other terms & conditions of the RFP.

Bank also reserves the right to continue or discontinue the availment of product / services without assigning any reason, in case of its merger or amalgamation and the merged or amalgamated entity shall have the same rights.

63. Signing of Contract

The successful bidder(s) to be called as bidder, shall be required to enter into an Agreement with the Bank, within 21 days of the award of the work order (when provided) or within such extended period as may be specified by the bank.

64. Checklist for Submission

#	Particulars	Bidders Remark Yes/No
1	Certificate of incorporation	
2	GSTN Registration Certificate	
3	Copy of Audited Balance sheets of last three years 2023-24, 2024-25 & 2025-26 of the bidder	
4	CA certificate for three years average turnover for financial years 2023-24, 2024-25 & 2025-26 of the bidder	
5	CA certificate for operating profit for last three financial years 2023-24, 2024-25 & 2025-26 of the bidder	

#	Particulars	Bidders Remark Yes/No
6	CA certificate for net worth for last three financial years 2023-24, 2024-25 & 2025-26 of the bidder	
7	Self-declaration on Company's letter head should not have been Blacklisted /debarred/ by any Govt. / IBA/RBI/PSU /PSE/ or Banks, Financial institutes for any reason or non-implementation/ delivery of the order. Self-declaration to that effect should be submitted along with the technical bid.	
8	Self-declaration on Company's letter head Bidder/OEM should not have any pending litigation or any dispute in the last five years, before any court of law between the Bidder or OEM and the Bank regarding supply of goods/services.	
9	Self-declaration by the Authorized Signatory for not have filed for bankruptcy in any country including India on company letter head	
10	Self-declaration on Company's letter-head for not having • NPA with any Bank /financial institutions in India • Any case pending or otherwise, with any organization across the globe which affects the credibility of the Bidder in the opinion of Central Bank of India to service the needs of the Bank Pending	
11	Self-declaration by the Authorized Signatory for having support / service center or having support arrangement in Mumbai and Hyderabad.	
12	Certified copy of the registration certificate if the bidder is from a country which shares a land border with India	
13	Documents as mentioned in Eligibility Criteria of the RFP	
14	Copy of the power of Attorney of signing authority / executor	
15	All Annexures of RFP	

65. Annexure-1 Bill of Material

Bidder needs to provide the compliance on below Bill of Materials on Bidder's letter head.

Sr. No.	Particulars	Frequency	Number of Instance	Price per Instance (INR)	GST	Total Price for One Instance
1	Vulnerability Assessment	Quarterly/As Applicable/As per Bank's Requirement	8			
2	Penetration Testing	Half Yearly/As Applicable/As per Bank's Requirement	4			
3	Web & Application Security	Half Yearly/As Applicable/As per Bank's Requirement	4			
4	Code Review & Secure Coding Practices	Annually/As Applicable/As per Bank's Requirement	4			
5	Mobile Application Security Assessment	Half Yearly/As Applicable/As per Bank's Requirement	4			
6	Security and Network Architecture Review	Half Yearly/As Applicable/As per Bank's Requirement	4			
7	Secure Configuration Documentation & Review	Annually/As Applicable/As per Bank's Requirement	4			
8	Cyber Security Tools/Solutions including Network Security Tools/Solutions Configuration Assessment	Half Yearly/As Applicable/As per Bank's Requirement	4			
9	AI Technology Vulnerability Management	Quarterly/As Applicable/As per Bank's Requirement	8			
10	Red Teaming	Quarterly/As Applicable/As per Bank's Requirement	8			

11	Digital Forensic Services	As and when required/As Applicable/As per Bank's Requirement	Need Basis			
12	ISO 27001 &/ ISO 22301 Consulting	Annually/As Applicable/As per Bank's Requirement	2			
13	ISO 42001 Certification Preparation	Annually/As Applicable/As per Bank's Requirement	2			
14	Cyber Security Maturity Assessment	Annually/As Applicable/As per Bank's Requirement	2			
15	KRI/ KPI Reviews	Quarterly/As Applicable/As per Bank's Requirement	8			
16	Regulatory Compliance Review	Half Yearly/As Applicable/As per Bank's Requirement	4			
17	Documentation – Policy, Processes, Procedure Creation/Review/ Modification etc.	Half Yearly/As Applicable/As per Bank's Requirement	4			
18	SOC Review	Half Yearly/As Applicable/As per Bank's Requirement	4			
19	Cyber Resilience Preparedness	Half Yearly/As Applicable/As per Bank's Requirement	4			
20	ISD Resource Assessment and Future Resource Planning	One Time Activity/As Applicable/As per Bank's Requirement	ONE			
21	Rate for additional requirement for each of the above line items (except forensic services) to be mentioned separately by adding additional rows	NA	ONE			

	(Payment of such additional requirements will be made by Bank as per the actuals after availing the service and its completion signoff)					
	Grand Total (for priced line items)					

**Rate quoted should be inclusive of taxes and charges except GST. GST will be payable actual and on submission of original invoice / receipt.*
**Rate quoted in GeM portal should be inclusive of GST.*

- The Bidder is expected to quote for all items required for fully complying with the requirements of the RFP.
- The Bank is not responsible for any omission/skip of any component required for complying with the RFP requirement and bidder will have to fulfil the entire requirement without any additional cost to Bank.
- Bank is not responsible for any arithmetic errors in the commercial bid details submitted by the bidder.
- The bidder may insert any additional line item as applicable based on the solution offered by the bidder.
- **Bidder must quote as per format of the bill of material only and masked replica of the bill of material should be enclosed in the technical bid without any commercial value. Failure to comply with submission of masked replica of BOM on the letterhead of the bidder, duly signed and sealed by an authorized signatory will be liable to rejection of the bid.**
- All amount in bill of material should be in INR only.
- Any additional number of items (Software, Hardware, FMS etc.) and services to be procured by the Bank in future shall be on pro-rata basis on the rates provided in the bill of material.
- If the bidder has not quoted for any line item mentioned in the bill of material, it will deemed considered that bidder has factored the cost for the item and no additional charges will be paid by the Bank, other than one mentioned in the bill of material.

Signature

Name:
Designation:
Seal of Company

Date:

66. Annexure 2: Conformity Letter

Pro forma of letter to be given by all the bidders participating in RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank on their official letter-head

Date :

To,

CISO,
Central Bank Of India,
Information Security Department,
Plot no-26, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,

Sub: RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank

Tender No. GEM/2026/B/8006355

Further to our proposal dated _____, in response to the RFP document (hereinafter referred to as "RFP DOCUMENT") issued by Central Bank of India ("Bank") we hereby covenant, warrant and confirm as follows:

We hereby agree to comply with all the terms and conditions / stipulations as contained in the RFP document and the related addendums and other documents including the changes made to the original tender documents issued by the Bank.

The Bank is not bound by any other extraneous matters or deviations, even if mentioned by us elsewhere either in our proposal or any subsequent deviations sought by us, whether orally or in writing, and the Bank's decision not to accept any such extraneous conditions and deviations will be final and binding on us.

Yours faithfully,

Authorized Signatory

Designation

Company Name

67. Annexure 3: Bidder's Information

#	Particulars	Details
1.	Name of bidder	
2.	Constitution	
3.	Address with Pin code	
4.	Authorized Person for bid	
5.	Contact Details (Mail id & Mob No)	
6.	Years of Incorporation	
7.	Number of years of existence	
8.	Annual Turnover (In Rs.) 2023-24 – 2024-25 – 2025-26 -	
9.	Operating Profits (In Rs.) 2023-24 – 2024-25 — 2025-26 -	
10.	Net Worth (In Rs.) 2023-24 – 2024-25 – 2025-26 -	
11.	Whether OEM or authorized vendor	
12.	Number of service outlets across India	
13.	Good and Service Tax Number	
14.	Income Tax Number	
15.	Name and Address of OEMs	
16.	Brief Description of after sales service facilities available with the bidder.	
17.	Whether all RFP terms & conditions complied with.	

Signature

Name:
Designation:
Seal of Company

Date:

68. Annexure 4: Letter for Conformity of Product as per RFP

Pro forma of letter to be given by all the bidders participating in RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank on their official letter-head

Date :

To,

CISO,
Central Bank Of India
Information Security Department,
Plot no-26, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,

Sub: RFP for Appointment of cyber security consultant for various consultancy services

Tender No GEM/2026/B/8006355

We submit our Bid Document herewith. If our Bid for the above job is accepted, we undertake to enter into and execute at our cost, when called upon by the bank to do so, a contract in the prescribed form. Unless and until a formal contract is prepared and executed, this bid together with your written acceptance thereof shall constitute a binding contract between us.

We understand that any deviations mentioned elsewhere in the bid will not be considered and evaluated by the Bank. We also agree that the Bank reserves its right to reject the bid, if the bid is not submitted in proper format as per subject RFP.

We undertake that product and services supplied shall be as per the:-

Compliance	Compliance (Yes/ No)	Remarks
Terms & Conditions		
Scope of Work		
Technical Specifications		
Eligibility Criteria		

Signature

Name:
Designation:
Seal of Company

Date:

69. ANNEXURE 5: UNDERTAKING FOR ACCEPTANCE OF TERMS OF RFP

Pro forma of letter to be given by all the bidders participating in RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank on their official letter-head

Date :

To,

CISO,
Central Bank Of India
Information Security Department,
Plot no-26, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,

Sub: RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank

Tender No : GEM/2026/B/8006355

With reference to RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank:

We understand that Bank shall be placing Order to the Successful Bidder exclusive/inclusive of taxes only.

1. We confirm that in case of invocation of any Bank Guarantees submitted to the Bank, we will pay applicable GST on Bank Guarantee amount.
2. We are agreeable to the payment schedule as per "Payment Terms" of the RFP.
3. We here by confirm to undertake the ownership of the subject RFP.
4. We hereby undertake to provide latest product/ software with latest version as mentioned in the RFP. The charges for the above have been factored in Bill of Material (BOM), otherwise the Bid is liable for rejection. We also confirm that we have not changed the format of BOM.
5. We undertake to provide SBOM and CBOM as and when required by Bank in Bank's prescribed format.

Signature

Name:
Designation:
Seal of Company

Date:

70. ANNEXURE 6: INTEGRITY PACT

Integrity Pact

Between

Central Bank of India hereinafter referred to as "The Principal",

And

…… hereinafter referred to as "The Bidder/ Contractor"

Preamble

The Principal intends to award, under laid down organizational procedures, contract/s for……The Principal values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness / transparency in its relations with its Bidder(s) and / or Contractor(s).

In order to achieve these goals, the Principal will appoint an Independent External Monitor (IEM), who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

Section 1 – Commitments of the Principal

(1.) The Principal commits itself to take all measures necessary to prevent corruption and to observe the following principles:-

a. No employee of the Principal, personally or through family members, will in connection with the tender for , or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

b. The Principal will, during the tender process treat all Bidder(s) with equity and reason. The Principal will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential / additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution.

c. The Principal will exclude from the process all known prejudiced persons.

(2) If the Principal obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

Section 2 – Commitments of the Bidder(s)/ contractor(s)

(1) The Bidder(s)/ Contractor(s) commit themselves to take all measures necessary to prevent corruption. He commits himself to observe the following principles during his participation in the tender process and during the contract execution.

a. The Bidder(s)/ Contractor(s) will not, directly or through any other person or firm, offer, promise or give to any of the Principal's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract.

b. The Bidder(s)/ Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelisation in the bidding process.

c. The Bidder(s)/ Contractor(s) will not commit any offence under the relevant IPC/PC Act; further the Bidder(s)/ Contractor(s) will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

d. The Bidder(s)/Contractors(s) of foreign origin shall disclose the name and address of the Agents/representatives in India, if any. Similarly the Bidder(s)/Contractors(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any. Further details as mentioned in the "Guidelines on Indian Agents of Foreign Suppliers" shall be disclosed by the Bidder(s)/Contractor(s).Further, as mentioned in the Guidelines all the payments made to the Indian agent/representative have to be in Indian Rupees only.

e. The Bidder(s)/ Contractor(s) will, when presenting his bid, disclose any and all payments he has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract.

(2) The Bidder(s)/ Contractor(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section 3- Disqualification from tender process and exclusion from future contracts

If the Bidder(s)/Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or in any other form such as to put his reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s)/Contractor(s) from the tender process or take action as per the procedure mentioned in the "Guidelines on Banning of business dealings".

Section 4 – Compensation for Damages

(1) If the Principal has disqualified the Bidder(s) from the tender process prior to the award according to Section 3, the Principal is entitled to demand and recover the damages equivalent to Earnest Money Deposit/ Bid Security.

(2) If the Principal has terminated the contract according to Section 3, or if the Principal is entitled to terminate the contract according to Section 3, the Principal shall be entitled to

demand and recover from the Contractor liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee.

Section 5 – Previous Transgression

(1) The Bidder declares that no previous transgressions occurred in the last three years with any other Bank in any country conforming to the anti-corruption approach or with any Public Sector Enterprise in India that could justify his exclusion from the tender process.

(2) If the Bidder makes incorrect statement on this subject, he can be disqualified from the tender process or action can be taken as per the procedure mentioned in "Guidelines on Banning of business dealings".

Section 6 – Equal treatment of all Bidders / Contractors / Subcontractors

(1) The Bidder(s)/ Contractor(s) undertake(s) to demand from his subcontractors a commitment in conformity with this Integrity Pact.

(2) The Principal will enter into agreements with identical conditions as this one with all Bidders and Contractors.

(3) The Principal will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

Section 7 – Criminal charges against violating Bidder(s) / Contractor(s) / Subcontractor(s)

If the Principal obtains knowledge of conduct of a Bidder, Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if the Principal has substantive suspicion in this regard, the Principal will inform the same to the Chief Vigilance Officer.

Section 8 – Independent External Monitor / Monitors

(1) The Principal appoints competent and credible Independent External Monitor for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.

(2) The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. It will be obligatory for him to treat the information and documents of the Bidders/Contractors as confidential. He reports to the Chairman & Managing Director, CENTRAL BANK OF INDIA.

(3) The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the Principal including that provided by the Contractor. The Contractor will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/ Contractor(s)/ Subcontractor(s) with confidentiality. In case of sub-contracting, the Principal Contractor shall take all

responsibility of the adoption of Integrity Pact by the sub-contractor. In case of sub-contracting, the Principal Contractor shall take the responsibility of the adoption of the Integrity Pact by the sub-contractor.

(4) The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Contractor. The parties offer to the Monitor the option to participate in such meetings.

(5) As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit nonbinding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action. Parties to this agreement agree that they shall not approach the courts while representing the matter to IEM and will await IEM's decision in the matter. Parties to this agreement agree that they shall not approach the courts while representing the matter to IEM and will await IEM's decision in the matter.

(6) The Monitor will submit a written report to the Chairman & Managing Director, CENTRAL BANK OF INDIA within 8 to 10 weeks from the date of reference or intimation to him by the Principal and, should the occasion arise, submit proposals for correcting problematic situations.

(7) If the Monitor has reported to the Chairman & Managing Director CENTRAL BANK OF INDIA, a substantiated suspicion of an offence under relevant IPC/ PC Act, and the Chairman & Managing Director CENTRAL BANK OF INDIA has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

(8) The word „Monitor" would include both singular and plural.

Section 9 – Pact Duration

This Pact begins when both parties have legally signed it. It expires for the Contractor 12 months after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded.

If any claim is made / lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged / determined by Chairman & Managing Director of CENTRAL BANK OF INDIA.

Section 10 – Other provisions

(1) This agreement is subject to Indian Law. Place of performance and jurisdiction is the Registered Office of the Principal, i.e. Mumbai.

(2) Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.

(3) If the Contractor is a partnership or a consortium, this agreement must be signed by all partners or consortium members.

(4) Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

(5) In the event of any contradiction between the Integrity Pact and its Annexure, the Clause in the Integrity Pact will prevail."

Section 11- FALL CLAUSE

11.1. The BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER undertakes that it has not supplied/is not supplying same/exact product/systems or subsystems/services (i.e. same scope, deliverables, timelines, SLAs & pricing terms) at a price lower than that offered in the present bid to any other Bank or PSU or Government Department or to any other organization/entity whether or not constituted under any law and if it is found at any stage that similar product/systems or sub systems/services was supplied by the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER to any other Bank or PSU or Government Department or to any other organization/entity whether or not constituted under any law, at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER to the BUYER, if the contract has already been concluded.

Signed, Sealed and Delivered for the Principal	**Signed, Sealed and Delivered for the Bidder**
Signature: _____	Signature: _____
Name: _____	Name: _____
Designation: _____	Designation: _____
Address: _____	Address: _____
Company: _____	Company: _____
Date: _____	Date: _____
Company Seal	**Company Seal**
Witness I	**Witness II**
Signature: _____	Signature: _____
Name: _____	Name: _____
Designation: _____	Designation: _____

Address: _____	Address: _____
Company: _____	Company: _____
Date: _____	Date: _____

71. Annexure 7: Non-Disclosure Agreement

This Agreement made at _____, on this _____ day of _____ 2025

Between

_____ a company incorporated under the Companies Act, 1956/2013 having its registered office at _____ (hereinafter referred to as "-----" which expression unless repugnant to the context or meaning thereof be deemed to include its successors and assigns) of the ONE PART;

AND

CENTRAL BANK OF INDIA, a body corporate constituted under the Banking Companies (Acquisition & Transfer of Undertakings) Act, 1970 and having its head Office at Central Office, Chander Mukhi, Nariman Point, Mumbai – 400 021 (hereinafter referred to as "BANK" which expression unless repugnant to the context or meaning thereof be deemed to include its successors and assigns) of the OTHER PART

The …….bidder and BANK are hereinafter individually referred to as party and collectively referred to as "the Parties". Either of the parties which discloses or receives the confidential information is respectively referred to herein as Disclosing Party and Receiving Party.

WHEREAS:

The Parties intend to engage in discussions and negotiations concerning the establishment of a business relationship between them. In the course of such discussions and negotiations, it is anticipated that both the parties may disclose or deliver to either of the Parties certain or some of its trade secrets or confidential or proprietary information, for the purpose of enabling the other party to evaluate the feasibility of such business relationship (hereinafter referred to as "the Purpose").

NOW, THEREFORE, THIS AGREEMENT WITNESSETH AND IT IS HEREBY AGREED BY AND BETWEEN THE PARTIES HERETO AS FOLLOWS:

1. Confidential Information

"Confidential Information" means all information disclosed/ furnished by either of the parties to another Party in connection with the business transacted/to be transacted between the Parties and/or in the course of discussions and negotiations between them in connection with the Purpose. Confidential Information shall include customer data, any copy, abstract, extract, sample, note or module thereof.

Either of the Parties may use the Confidential Information solely for and in connection with the Purpose.

Notwithstanding the foregoing, "Confidential Information" shall not include any information which the Receiving Party can show: (a) is now or subsequently becomes legally and publicly available without breach of this Agreement by the Receiving Party, (b) was rightfully in the possession of the Receiving Party without any obligation of confidentiality prior to receiving it from the Disclosing Party, (c) was rightfully obtained by the Receiving Party from a source other than the Disclosing Party without any obligation of confidentiality, or (d) was developed by or for the Receiving Party independently and without reference to any Confidential Information and such independent development can be shown by documentary evidence.

2. Non-Disclosure

The Receiving Party shall not commercially use or disclose any Confidential Information or any materials derived there from to any other person or entity other than persons in the direct employment of the Receiving Party who have a need to have access to and knowledge of the Confidential Information solely for the Purpose authorized above. The Receiving Party may disclose Confidential Information to its employees, consultants, auditors, sub-contractors ("Representatives") consultants only if such representatives has executed a Non-disclosure Agreement with the Receiving Party that contains terms and conditions that are no less restrictive than these. The Receiving Party shall take appropriate measures by instruction and written agreement prior to disclosure to such employees to assure against unauthorized use or disclosure. The Receiving Party agrees to notify the Disclosing Party immediately if it learns of any use or disclosure of the Disclosing Party's Confidential Information in violation of the terms of this Agreement. Further, any breach of non-disclosure obligations by such employees or consultants shall be deemed to be a breach of this Agreement by the Receiving Party and the Receiving Party shall be accordingly liable therefor.

Provided that the Receiving Party may disclose Confidential information to a court or governmental agency pursuant to an order of such court or governmental agency as so required by such order, provided that the Receiving Party shall, unless prohibited by law or regulation, promptly notify the Disclosing Party of such order and afford the Disclosing Party the opportunity to seek appropriate protective order relating to such disclosure.

3. Publications

Neither Party shall make news releases, public announcements, give interviews, issue or publish advertisements or publicize in any other manner whatsoever in connection with this Agreement, the contents / provisions thereof, other information relating to this Agreement, the Purpose, the Confidential Information or other matter of this Agreement, without the prior written approval of the other Party.

4. Term

This Agreement shall be effective from the date hereof and shall continue till establishment of business relationship between the Parties and execution of definitive agreements thereafter. Upon expiration or termination as contemplated herein the Receiving Party shall immediately cease rights to any and all disclosures or uses of Confidential Information; and at the request of

the Disclosing Party, the Receiving Party shall promptly return or destroy all written, graphic or other tangible forms of the Confidential Information and all copies, abstracts, extracts, samples, notes or modules thereof.

Notwithstanding anything to the contrary contained herein, the confidential information shall continue to remain confidential until it reaches the public domain in the normal course.

6. Title & Proprietary Rights

Notwithstanding the disclosure of any Confidential Information by the Disclosing Party to the Receiving Party, the Disclosing Party shall retain title and all intellectual property and proprietary rights in the Confidential Information. No license under any trademark, patent or copyright, or application for same which are now or thereafter may be obtained by such Party is either granted or implied by the conveying of Confidential Information. The Receiving Party shall not conceal, alter, obliterate, mutilate, deface or otherwise interfere with any trademark, trademark notice, copyright notice, confidentiality notice or any notice of any other proprietary right of the Disclosing Party on any copy of the Confidential Information, and shall reproduce any such mark or notice on all copies of such Confidential Information. Likewise, the Receiving Party shall not add or emboss its own or any other any mark, symbol or logo on such Confidential Information.

7. Return of Confidential Information

Upon written demand of the Disclosing Party, the Receiving Party shall (i) cease using the Confidential Information, (ii) return the Confidential Information and all copies, abstract, extracts, samples, notes or modules thereof to the Disclosing Party within seven (7) days after receipt of notice, and (iii) upon request of the Disclosing Party, certify in writing that the Receiving Party has complied with the obligations set forth in this paragraph. The obligation under this clause will not apply where it is necessary to retain any confidential information for the purpose as required by the law or for internal auditing purposes or electronic data stored due to automatic archiving or backup procedures.

8. Remedies

The Receiving Party acknowledges that if the Receiving Party fails to comply with any of its obligations hereunder, the Disclosing Party may suffer immediate, irreparable harm for which monetary damages may not be adequate. The Receiving Party agrees that, in addition to all other remedies provided at law or in equity, the Disclosing Party shall be entitled to injunctive relief hereunder.

9. Entire Agreement, Amendment and Assignment

This Agreement constitutes the entire agreement between the parties relating to the matters discussed herein and supersedes any and all prior oral discussions and/or written correspondence or agreements between the parties. This Agreement may be amended or modified only with the mutual written consent of the parties. Neither this Agreement nor any right granted hereunder shall be assignable or otherwise transferable.

10. Governing Law and Jurisdiction

The provisions of this Agreement shall be governed by the laws of India. The disputes, if any, arising out of this Agreement shall be submitted to the jurisdiction of the courts/tribunals in Mumbai.

11. General

The Receiving Party shall not reverse-engineer, decompile, disassemble or otherwise interfere with any software disclosed hereunder. All Confidential Information is provided "as is". In no event shall the Disclosing Party be liable for the inaccuracy or incompleteness of the Confidential Information. None of the Confidential Information disclosed by the parties constitutes any representation, warranty, assurance, guarantee or inducement by either party to the other with respect to the fitness of such Confidential Information for any particular purpose or infringement of trademarks, patents, copyrights or any right of third persons.

12. Indemnity

The receiving party should indemnify and keep indemnified, saved, defended, harmless against any loss, damage, costs etc. incurred and / or suffered by the disclosing party arising out of breach of confidentiality obligations under this agreement by the receiving party, its officers, employees, agents or consultants.

In WITNESS THEREOF, the Parties hereto have executed these presents the day, month and year first hereinabove written:

Signed, Sealed and Delivered for the Principal	**Signed, Sealed and Delivered for the Bidder**
Signature: _____	Signature: _____
Name: _____	Name: _____
Designation: _____	Designation: _____
Address: _____	Address: _____
Company: _____	Company: _____
Date: _____	Date: _____
Company Seal	**Company Seal**
Witness I	**Witness II**
Signature: _____	Signature: _____
Name: _____	Name: _____
Designation: _____	Designation: _____
Address: _____	Address: _____
Company: _____	Company: _____

Date: _____	Date: _____

72. Annexure 8: Performance Bank Guarantee

To,

Central Bank of India

Mumbai

In consideration of Central Bank of India having Registered Office at Chandermukhi Building, Nariman Point, Mumbai 400 021 (hereinafter referred to as "Purchaser") having agreed to purchase of ---------- (hereinafter referred to as "Goods") from M/s ---------- (hereinafter referred to as "Contractor") on the terms and conditions contained in their agreement/purchase order No------- dt.---------- (hereinafter referred to as the "Contract") subject to the contractor furnishing a Bank Guarantee to the purchaser as to the due performance of the computer hardware, as per the terms and conditions of the said contract, to be supplied by the contractor and also guaranteeing the maintenance, by the contractor, of the computer hardware and systems as per the terms and conditions of the said contract;

1) We, ---------- (Bank) (hereinafter called "the Bank"), in consideration of the premises and at the request of the contractor, do hereby guarantee and undertake to pay to the purchaser, forthwith on mere demand and without any demur, at any time up to ---------- any money or moneys not exceeding a total sum of Rs---------(Rupees----------only) as may be claimed by the purchaser to be due from the contractor by way of loss or damage caused to or that would be caused to or suffered by the purchaser by reason of failure of computer hardware to perform as per the said contract, and also failure of the contractor to maintain the computer hardware and systems as per the terms and conditions of the said contract.

2) Notwithstanding anything to the contrary, the decision of the purchaser as to whether computer hardware has failed to perform as per the said contract, and also as to whether the contractor has failed to maintain the computer hardware and systems as per the terms and conditions of the said contract will be final and binding on the Bank and the Bank shall not be entitled to ask the purchaser to establish its claim or claims under this Guarantee but shall pay the same to the purchaser forthwith on mere demand without any demur, reservation, recourse, contest or protest and/or without any reference to the contractor. Any such demand made by the purchaser on the Bank shall be conclusive and binding notwithstanding any difference between the purchaser and the contractor or any dispute pending before any Court, Tribunal, Arbitrator or any other authority.

3) This Guarantee shall expire on ----------; without prejudice to the purchaser's claim or claims demanded from or otherwise notified to the Bank in writing on or before the said date i.e. --------- (this date should be date of expiry of Guarantee).

4) The Bank further undertakes not to revoke this Guarantee during its currency except with the previous consent of the purchaser in writing and this Guarantee shall continue to be enforceable till the aforesaid date of expiry or the last date of the extended period of expiry of

Guarantee agreed upon by all the parties to this Guarantee, as the case may be, unless during the currency of this Guarantee all the dues of the purchaser under or by virtue of the said contract have been duly paid and its claims satisfied or discharged or the purchaser certifies that the terms and conditions of the said contract have been fully carried out by the contractor and accordingly discharges the Guarantee.

5) In order to give full effect to the Guarantee herein contained, you shall be entitled to act as if we are your principal debtors in respect of all your claims against the contractor hereby Guaranteed by us as aforesaid and we hereby expressly waive all our rights of surety ship and other rights if any which are in any way inconsistent with the above or any other provisions of this Guarantee.

6) The Bank agrees with the purchaser that the purchaser shall have the fullest liberty without affecting in any manner the Bank's obligations under this Guarantee to extend the time of performance by the contractor from time to time or to postpone for any time or from time to time any of the rights or powers exercisable by the purchaser against the contractor and either to enforce or forbear to enforce any of the terms and conditions of the said contract, and the Bank shall not be released from its liability for the reasons of any such extensions being granted to the contractor for any forbearance, act or omission on the part of the purchaser or any other indulgence shown by the purchaser or by any other matter or thing whatsoever which under the law relating to sureties would, but for this provision have the effect of so relieving the Bank.

7) The Guarantee shall not be affected by any change in the constitution of the contractor or the Bank nor shall it be affected by any change in the constitution of the purchaser by any amalgamation or absorption or with the contractor, Bank or the purchaser, but will ensure for and be available to and enforceable by the absorbing or amalgamated company or concern.

8) This guarantee and the powers and provisions herein contained are in addition to and not by way of limitation or in substitution of any other guarantee or guarantees heretofore issued by us (whether singly or jointly with other banks) on behalf of the contractor heretofore mentioned for the same contract referred to heretofore and also for the same purpose for which this guarantee is issued, and now existing un-cancelled and we further mention that this guarantee is not intended to and shall not revoke or limit such guarantee or guarantees heretofore issued by us on behalf of the contractor heretofore mentioned for the same contract referred to heretofore and for the same purpose for which this guarantee is issued.

9) Any notice by way of demand or otherwise under this guarantee may be sent by special courier, telex, fax or registered post to our local address as mentioned in this guarantee.

10) Notwithstanding anything contained herein above:-

i) Our liability under this Bank Guarantee shall not exceed ₹--------(Rupees---------only);

ii) This Bank Guarantee shall be valid up to ----------;(date of expiry of PBG) and

iii) We are liable to pay the Guaranteed amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written claim or demand on or before--- ---------- (date of expiry of Guarantee plus claim period , if any)

iv) All your rights to bring legal action under this guarantee shall extinguish on…… (date one year from the date mentioned in point no. iii above)

11) The Bank has power to issue this Guarantee under the statute/constitution and the undersigned has full power to sign this Guarantee on behalf of the Bank.

Date this ---------- day of ---------- 2026 at ---------

For and on behalf of ---------- Bank.

sd/- ----------

73. Annexure 9: Bid Security (Earnest Money Deposit)

To,

CISO,
Central Bank Of India
Information Security Department,
Plot no-26, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Dear Sir,

In response to your invitation to respond to your RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank on their official letter-head, M/s _____having their registered office at _____ (hereinafter called the "Bidder") wishes to respond to the said Request for Proposal (RFP) and submit the proposal for as listed in the RFP document.

Whereas the "Bidder" has submitted the proposal in response to RFP, we, the _____ Bank having our head office _____ hereby irrevocably guarantee an amount of ₹ _____/- (Rupees _____Only) as bid security as required to be submitted by the, "Bidder" as a condition for participation in the said process of RFQ.

The Bid security for which this guarantee is given is liable to be enforced/ invoked:

1. If the Bidder withdraws his proposal during the period of the proposal validity; or

2. If the Bidder, having been notified of the acceptance of its proposal by the Bank during the period of the validity of the proposal fails or refuses to enter into the contract in accordance with the Terms and Conditions of the RFP or the terms and conditions mutually agreed subsequently. We undertake to pay immediately on demand to Central Bank of India the said amount without any reservation, protest, demur, or recourse. The said guarantee is liable to be invoked/ enforced on the happening of the contingencies as mentioned above and also in the RFP document and we shall pay the amount on any Demand made by Central Bank of India which shall be conclusive and binding on us irrespective of any dispute or difference raised by the Bidder.

Notwithstanding anything contained herein above:

1. Our liability under this Bank guarantee shall not exceed ₹ _____/- (Rupees _____Only)

2. This Bank guarantee will be valid up to _____; and

3. We are liable to pay the guarantee amount or any part thereof under this Bank

Guarantee only upon service of a written claim or demand by you on or before_____ (date of expiry of Guarantee plus claim period , if any)

4. All your rights to bring legal action under this guarantee shall extinguish on…… (date one year from the date mentioned in point no. iii above)

In witness whereof the Bank, through the authorized officer has sets its hand and stamp on this _____day of _____ at .

Yours faithfully,

For and on behalf of _____

Bank Authorised Official

74. Annexure 10: Bidder's Particulars

#	Particulars	
1.	Name of the Bidder	
2.	Address with E mail id, Mobile no. and Pin code	
3.	GST Number	
4.	Bank Details	
5.	PAN Number	
6.	Name of Authorised Person Mobile No: Landline No:	
7.	i. Email ID ii. Alternative Email ID	
8.	Details of EMD	BG/UTR/Reference No. date & Amount
9.	Exemption Certificate details (if applicable). Ex: MSE etc.	Please upload copy of the same along with details

Signature

Name:
Designation:
Seal of Company

Date:

75. ANNEXURE 11: NPA/PENDING LITIGATION/BLACKLISTING UNDERTAKING

Pro forma of letter to be given by all the bidders participating in RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank on their official letter-head

Date :
To,
CISO,
Central Bank Of India,
Information Security Department,
Plot no-26, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,

Sub: RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank

Tender No. GEM/2026/B/8006355

We _____(bidder name), hereby undertake that-

- We have not have been declared NPA by any Bank in India.
- Further, we do not have any pending case with any organization in India which affects our credibility to service the bank.
- Further, we are not blacklisted/debarred/ by any Govt. / IBA/RBI/PSU /PSE/ or Banks, Financial institutes for any reason including non-implementation/delivery of any order.

Yours faithfully,

Authorised Signatory

Designation

Bidder's corporate name

76. ANNEXURE 12: UNDERTAKING LETTER (LAND BORDER SHARING)

Pro forma of letter to be given by all the bidders participating in RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank on their official letter-head

Date :
To,
CISO,
Central Bank Of India,
Information Security Department,
Plot no-26, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,
Sub: RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank

Tender No. GEM/2026/B/8006355

Dear Sir/Madam,

We, M/s_____ are a private/ public limited company/ LLP/ firm <strike off whichever is not applicable> incorporated under the provisions of the Companies Act, 1956/2013, Limited Liability Partnership Act 2008/ Indian Partnership Act 1932, having our registered office at _____ (referred to as the "Bidder") are desirous of participating in the Tender Process in response to our captioned RFP and in this connection we hereby declare, confirm and agree as follows:

We, the Bidder have read and understood the contents of the RFP and Office Memorandum & the Order (Public Procurement No.1) both bearing no.F.No.6/18/2019/PPD of 23rd July 2020 issued by Ministry of Finance, Government of India on insertion of Rule 144 (xi) in the General Financial Rules (GFRs) 2017 and the amendments & clarifications thereto, regarding restrictions on availing/ procurement of goods and services, of any Bidder from a country which shares a land border with India and/ or sub-contracting to contractors from such countries.

In terms of the above and after having gone through the said amendments including in particular the words defined therein (which shall have the same meaning for the purpose of this Declaration cum Undertaking), we, the Bidder hereby declare and confirm that:

Strike off whichever is not applicable

1. "I/we have read the clause regarding restrictions on procurement from a bidder of the country which shares a land border with India; I/ we certify that _____ is not from such a country.
2. "I/we have read the clause regarding restrictions on procurement from a Bidder of a country which shares a land border with India; I/we certify that _____ is from such a country. I hereby certify that _____ fulfils all requirements in this regard and is eligible to be considered. [Valid registration by the Competent Authority is attached]"

Further, in case the work awarded to us, I/we undertake that I/we shall not subcontract any of assigned work under this engagement without the prior permission of Bank.

Further, we undertake that I/we have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India and on sub-contracting to contractors from such countries; I certify that our subcontractor is not from such a country or, if from such a country, has been registered with the Competent Authority and will not sub-contract any work to a contractor from such countries unless such contractor is registered with the Competent Authority. I hereby certify that our sub-contractor fulfils all requirements in this regard and is eligible to be considered. [Valid registration by the Competent Authority]"

We, hereby confirm that we fulfil all the eligibility criteria as per the office memorandum/ order mentioned above and RFP and we are eligible to participate in the Tender process. We also agree and accept that if our declaration and confirmation is found to be false at any point of time including after awarding the contract, Bank shall be within its rights to forthwith terminate the contract/ bid without notice to us and initiate such action including legal action in accordance with law. Bank shall also be within its right to forfeit the security deposits/ earnest money provided by us and also recover from us the loss and damages sustained by the Bank on account of the above.

This declaration cum Undertaking is executed by us through our Authorized signatory/ ies after having read and understood the Office Memorandum and Order including the words defined in the said order.

Dated this _____ by _____20__

Yours faithfully,

Authorized Signatory
Name:
Designation:
Bidder's Corporate Name:
Address:
Email & Phone No.:

List of documents enclosed:

1. Copy of Certificate of valid registration with the Competent Authority (strike off if not applicable
2. _____
3. _____
4. _____

77. ANNEXURE 13: COVER LETTER

Pro forma of letter to be given by all the bidders participating in RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank on their official letter-head

Date :
To,
CISO,
Central Bank Of India,
Information Security Department,
Plot no-26, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,
Sub: RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank

Tender No. GEM/2026/B/8006355

1. Having examined the Scope Documents including all Annexures, the receipt of which is hereby duly acknowledged, we, the undersigned offer to supply, deliver, install and maintain all the items mentioned in the 'Request for Proposal' and the other schedules of requirements and services for your bank in conformity with the said Scope Documents in accordance with the schedule of Prices indicated in the Price Bid and made part of this Scope.
2. If our Bid is accepted, we undertake to abide by all terms and conditions of this Scope and also to comply with the delivery schedule as mentioned in the Scope Document.
3. We agree to abide by this bid Offer for 120 days from date of bid (Commercial Bid) opening and our Offer shall remain binding on us which may be accepted by the Bank any time before expiry of the offer.
4. This Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.
5. We undertake that in competing for and if the award is made to us, in executing the subject Contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".
6. We certify that we have provided all the information requested by the bank in the format prescribed for. We also understand that the bank has the exclusive right to reject this offer in case the bank is of the opinion that the required information is not provided or is provided in a different format.

Authorised Signatory

(Name: Contact Person, Phone No., Fax, E-mail)

(This letter should be on the letterhead of the Bidder duly signed by an authorized signatory)

78. Annexure 14: Pre-bid Query Format

Pro forma of letter to be given by all the bidders participating in RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank on their official letter-head and soft copy format (such as Excel/CSV) to the Bank for ease of consolidation and review.

Queries:

Sr. No.	Page # (Only Numeric)	RFP Point / Section # (Alpha Numeric only)	Query (Detailed Query)	Request (if any)	Banks Response (Bidder Should not fill in this column)
1					
2					
3					
4					
5					
6					
7					
8					
9					

Date:

Authorised Signatory & Stamp

(Name: Contact Person, Phone No., Fax, E-mail)

79. Annexure 15: Eligibility Criteria Compliance

Bidder needs to comply with the eligibility criterion mentioned below. Non-compliance with any of these criterions would result in outright rejection of bidder's proposal. Bidder is expected to provide proof for each of the points for eligibility evaluation criteria. Any credential detail not accompanied by required relevant proof documents will not be considered for evaluation. All credential letters should be appropriately bound, labeled and segregated in the respective areas. There is no restriction on the number of credentials a bidder can provide.

The decision of Bank pertaining to Eligibility Criteria evaluation would be final and binding on all the bidders. Bank may accept or reject an offer without assigning any reason whatsoever.

Date :
To,
CISO,
Central Bank Of India,
Information Security Department,
Plot no-26, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,
Sub: RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank

Tender No. GEM/2026/B/8006355

We Certify that we comply with below listed Eligibility Criteria as per the requirement of RFP, the decision of Bank pertaining to Eligibility Criteria evaluation would be final and binding on us. Bank may accept or reject an offer without assigning any reason whatsoever.

#	Eligibility Criteria for Bidder / OEM	Documents to be submitted	Compliance (Y / N)
GENERAL			
1.	The bidder must be a Registered company under Indian Companies Act. 1956/2013 or LLP/Partnership firm and should have been in existence for a **minimum period of 5 years in India**, as on date of submission of bid.	Copy of the Certificate of Incorporation issued by Registrar of Companies/Registrar of firms and full address of the registered office of the bidder	

2.	The bidder must be registered under G.S.T and/or tax registration in state where bidder has a registered office.	Proof of registration with GSTIN	
FINANCIAL			
3.	The bidder must have minimum average annual turnover **in India of Rs. 500 crores** each year in the last three financial years (i.e. 2023-24, 2024-25,2025-2026).	Copy of Audited Balance Sheet and Certificate of the Chartered Accountant for the last three financial years (i.e. 2023-24, 2024-25,2025-2026)	
4.	The bidder must have made **operating profit in at least two financial years** out of last three financial years (i.e. 2023-24, 2024-25,2025-2026)	Copy of Audited Balance Sheet and Certificate of the Chartered Accountant for the last three financial years (i.e. 2023-24, 2024-25,2025-2026)	
5.	The bidder must have a **positive net worth in last three financial years** (i.e. 2023-24, 2024-25,2025-2026)	Copy of Audited Balance Sheet and Certificate of the Chartered Accountant for the last three financial years (i.e. 2023-24, 2024-25,2025-2026)	
DEFAULT			
6.	At the time of bidding, the Bidder must not have been blacklisted/debarred/ by any Govt. / IBA/RBI/PSU /PSE/ or Banks, Financial institutes for any reason including non-implementation/delivery of the order. Self-declaration to that effect should be submitted along with the technical bid.	Undertaking on Company's letter head	
7.	At the time of bidding, there must not have been any pending litigation or any legal dispute, before any court of law between	Submit the undertaking self-declaration on Company's letter head	

	the Bidder or OEM(if any) and the Bank.		
8.	The bidder must not have NPA with any Bank /financial institutions in India Any case pending or otherwise, with any organization in India which affects the credibility of the Bidder in the opinion of Central Bank of India to service the needs of the Bank may be a ground for rejection of the bid at the discretion of the Bank.	Submit self-declaration on Company's letter head.	
9.	The bidder must have presence in Mumbai and Hyderabad.	Submit the undertaking self-declaration on Bidder's letter head	
10.	If the bidder is from a country which shares a land border with India, the bidder must be registered with the Competent Authority.	Certified copy of the registration certificate	
EXPERIENCE			
11	The bidder must be currently **empanelled with CERT-In** as Information Security Auditing Organization by **10 years**, out of which **last 4 years** should be on continuous basis.	Certificate / Empanelment letter / Equivalent letter issued by Cert-In	
12.	The Bidder must have experience and expertise of each of the service as mention below in at least any one **Schedule Commercial Bank with minimum 2000 Branches in India during last 5 years**. The Project must be of **min. 1 year**	Letter of acceptance (LoA)/ purchase order along with completion certificate or any relevant document acceptable to Bank/ work order/ contract/ completion certificate Deployment Certificate issued by client to the bidder/Particulars confirming relevant experience.	

	duration and of min. **Rs. 2 Lacs value per line item.** 1. Vulnerability Assessment 2. Penetration Testing 3. Web & Application Security 4. Code Review and Secure Coding Practices 5. Mobile Application Security Assessment 6. Red Teaming 7. Digital Forensic Services 8. Regulatory Compliance Review 9. Documentation – Policy, Processes, Procedure Creation/Review/ Modification etc. **(Minimum one experience in each of the service mentioned above is mandatory)**		
13.	The bidder must **have minimum 70 permanent employees in India** as on date of submission of bids. **Out of 70, min. 20 employees** should mandatorily have either of the • CISA • CISM • CISSP • CRISC	Undertaking on bidder letter head needs to submit along with certification details and relevant evidence.	

	• OSCP certification and remaining employees may have any of the below certifications for each employee (Certificate should be in unexpired status and live up to date of submission of bids) • Certified PCI-DSS professional • ISO 27001 LA • ISO 27001 LI • CRTP • CHFI • CIAC • SSCP • ECSA • CEH Note: The employee having multiple certificates shall be counted one resource only		

Authorised Signatory

(Name: Contact Person, Phone No., Fax, E-mail)
(This letter should be on the letterhead of the Bidder duly signed by an authorized signatory)

80. ANNEXURE 16: SELF DECLARATION FOR COMPLIANCE TO RBI MASTER DIRECTION ON OUTSOURCING OF IT SERVICES

(on Bidder's letterhead)

Date :
To,
CISO,
Central Bank Of India,
Information Security Department,
Plot no-26, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,
Sub: RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank

Tender No. GEM/2026/B/8006355

We, M/s_____ hereby state that we have gone through the RBI Master Circular: RBI/2023-24/102 DoS.CO.CSITEG/SEC.1/31.01.015/2023-24 dated 10.04.2023 and subsequent circular/guidelines regarding Master Direction on Outsourcing of Information Technology Services and we hereby state that we comply to all the directions and clauses as stated in the aforesaid circular. We along with the resources deployed by us and services provided by us, will also ensure compliance of all the clauses and directions of the aforesaid circular throughout the period of the contract.

Date: _____

Place: _____

Authorised Signatory & Stamp

(Name: Contact Person, Phone No., Fax, E-mail)

81. Annexure 17: GOI Guidelines for preference to Make in India

Government has issued Public Procurement (Preference to Make in India) [PPP-MII] Order 2017 vide the Department for Promotion of Industry and Internal Trade (DPIIT) Order No.P45021/2/2017-B.E.-II dated 15.06.2017 and subsequent revisions vide Order No. 45021/2/2017-PP(BE-II) dated 16-9-2020 to encourage 'Make in India' and to promote manufacturing and production of goods, services and works in India with a view to enhancing income and employment.

It is clarified that for all intents and purposes, the latest revised order i.e. the order dated 169-2020 shall be applicable being revised Order of the original order i.e. Public Procurement (Preference to Make in India) [PPP-MII] Order 2017 dated 15-6-2017.

The salient features of the aforesaid Order are as under:

1) Class-I Local supplier - a supplier or service provider, whose goods, services or works offered for procurement, has local content equal to or more than 50%.

2) Class-II Local supplier - a supplier or service provider, whose goods, services or works offered for procurement, has local content equal to or more than 20% but less than 50%.

3) Non-Local supplier - a supplier or service provider, whose goods, services or works offered for procurement, has local content less than or equal to 20%.

4) The margin of purchase preference shall be 20 %., Margin of purchase preference means the maximum extent to which the price quoted by a local supplier may be above the L1 for the purpose of purchase preference.

5) "Minimum Local content" for the purpose of this RFP, the 'local content' requirement to categorize a supplier as 'Class-I local supplier' is minimum 50%. For 'Class-II local supplier', the 'local content' requirement is minimum 20%. If Nodal Ministry/Department has prescribed different percentage of minimum 'local content' requirement to categorize a supplier as 'Class-I local supplier'/ 'Class-II local supplier', same shall be applicable.

Verification of Local contents:

The local supplier at the time of submission of bid shall be required to provide a certificate from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content as per Annexure 5A. Local content certificate shall be issued based upon the procedure for calculating the local content /domestic value addition on the basis of notification bearing no. F. No.33(1) /2017-IPHW dated 14-9-2017 issued by Ministry of Electronics and Information Technology read with Public Procurement (Preference to Make in India) Order 2017 Revised vide the Department for Promotion of Industry and Internal Trade (DPIIT) Order No.P-45021/2/2017-B.E.-II dated 16-09-2020.

False declaration will be in breach of the Code of Integrity under Rule 175(i)(h) of the General Financial Rules for which a bidder or its successors can be debarred for up to two years as per rule 151 of the General Financial Rules along with such other actions may be permissible under law.

A supplier who has been debarred by any procuring entity for violation of this order shall not be eligible for preference under this order for procurement by any other procuring entity for the duration of the debarments. The debarment for such other procuring entities shall take effect prospectively from the date on which it comes to the notice of other procurement entities in the manner prescribed under order No P-45021/2/2017-PP(BE- II) dated 16-092020, para 9(h).
Note:
a) Bidder has to submit the Make in India Class-I / Class-II local supplier certificate as per attached format.

b) Bidder has to submit proposal for all line Items.

c) Any change in classification of Class-I and Class-II, Bidder may submit any change in class level for consideration in subsequent phases.

Purchase Preference:
1) Subject to the provisions of this Order and to any specific instructions issued by the Nodal Ministry or in pursuance of this Order, purchase preference shall be given to 'Class-I local supplier' in procurements undertaken by procuring entities in the manner specified here under,

2) In the procurements of goods or works, which are divisible in nature, the 'Class-I local supplier' shall get purchase preference over 'Class-II local supplier' as well as 'Non-local supplier', as per following procedure:
• Among all qualified bids, the lowest bid will be termed as L1. If L1 is 'Class-I local supplier', the contract for full quantity will be awarded to L1.

• If L1 bid is not a 'Class-I local supplier', 50% of the order quantity shall be awarded to L1. Thereafter, the lowest bidder among the 'Class-I local supplier' will be invited to match the L1 price for the remaining 50% quantity subject to the Class-I local supplier's quoted price falling within the margin of purchase preference, and contract for that quantity shall be awarded to such 'Class-I local supplier' subject to matching the L1 price. In case such lowest eligible 'Class-I local supplier' fails to match the L1 price or accepts less than the offered quantity, the next higher 'Class-I local supplier' within the margin of purchase preference shall be invited to match the L1 price for remaining quantity and so on, and contract shall be awarded accordingly. In case some quantity is still left uncovered on Class-I local suppliers, then such balance quantity may also be ordered on the L1 bidder.
3) In the procurements of goods or works, which are not divisible in nature, and in procurement of services where the bid is evaluated on price alone, the 'Class-I local supplier' shall get purchase preference over 'Class-II local supplier' as well as 'Non-local supplier', as per following procedure:
• Among all qualified bids, the lowest bid will be termed as L1. If L1 is 'Class-I local supplier', the contract will be awarded to L1.

• If L1 is not 'Class-I local supplier', the lowest bidder among the 'Class-I local supplier', will be invited to match the L1 price subject to Class-I local supplier's quoted price falling within the margin of purchase preference, and the contract shall be awarded to such 'Class-I local supplier' subject to matching the L1 price.
• In case such lowest eligible 'Class-I local supplier' fails to match the L1 price, the 'Class- I local supplier' with the next higher bid within the margin of purchase preference shall be invited to match the L1 price and so on and contract shall be awarded accordingly. In case none of the

'Class-I local supplier' within the margin of purchase preference matches the L1 price, the contract may be awarded to the L1 bidder.
4) "Class-2 local supplier" will not get purchase preference in any procurement, undertaken by procuring entities.

All others terms and condition are as per order no. No. P-45021/2/2017-PP (BE-II) dated: 16th September 2020.

82. ANNEXURE 18: GUIDELINES ON BANNING OF BUSINESS DEALING

GUIDELINES FOR INDIAN AGENTS OF FOREIGN SUPPLIERS

1.0 There shall be compulsory registration of agents for all Global (Open) Tender and Limited Tender. An agent who is not registered with CENTRAL BANK OF INDIA shall apply for registration in the prescribed Application –Form.

1.1 Registered agents will file an authenticated Photostat copy duly attested by a Notary Public/Original certificate of the principal confirming the agency agreement and giving the status being enjoyed by the agent and the commission/remuneration/salary/ retainer ship being paid by the principal to the agent before the placement of order by CENTRAL BANK OF INDIA.

1.2 Wherever the Indian representatives have communicated on behalf of their principals and the foreign parties have stated that they are not paying any commission to the Indian agents, and the Indian representative is working on the basis of salary or as retainer, a written declaration to this effect should be submitted by the party (i.e. Principal) before finalizing the order

2.0 DISCLOSURE OF PARTICULARS OF AGENTS/ REPRESENTATIVES IN INDIA. IF ANY.

2.1 Tenderers of Foreign nationality shall furnish the following details in their offer:

2.1.1 The name and address of the agents/representatives in India, if any and the extent of authorization and authority given to commit the Principals. In case the agent/representative be a foreign Bank, it shall be confirmed whether it is real substantial Bank and details of the same shall be furnished.

2.1.2 The amount of commission/remuneration included in the quoted price(s) for such agents/representatives in India.

2.1.3 Confirmation of the Tenderer that the commission/ remuneration if any, payable to his agents/representatives in India, may be paid by CENTRAL BANK OF INDIA in Indian Rupees only.

2.2 Tenderers of Indian Nationality shall furnish the following details in their offers:

2.2.1 The name and address of the foreign principals indicating their nationality as well as their status, i.e, whether manufacturer or agents of manufacturer holding the Letter of Authority of the Principal specifically authorizing the agent to make an offer in India in response to tender either directly or through the agents/representatives.

2.2.2 The amount of commission/remuneration included in the price (s) quoted by the Tenderer for himself.

2.2.3 Confirmation of the foreign principals of the Tenderer that the commission/remuneration, if any, reserved for the Tenderer in the quoted price (s), may be paid by CENTRAL BANK OF

INDIA in India in equivalent Indian Rupees on satisfactory completion of the Project or supplies of Stores and Spares in case of operation items .

2.3 In either case, in the event of contract materializing, the terms of payment will provide for payment of the commission /remuneration, if any payable to the agents/representatives in India in Indian Rupees on expiry of 90 days after the discharge of the obligations under the contract.

2.4 Failure to furnish correct and detailed information as called for in paragraph-2.0 above will render the concerned tender liable to rejection or in the event of a contract materializing, the same liable to termination by CENTRAL BANK OF INDIA. Besides this there would be a penalty of banning business dealings with CENTRAL BANK OF INDIA or damage or payment of a named sum.

Sr. Contents

1. Introduction

2. Scope

3. Definitions

4. Initiation of banning / suspension

5. Suspension of business dealing

6. Ground on which banning of business dealings can be initiated

7. Banning of business dealings

8. Removal from list of approved agencies –suppliers/contractors

9. Show-cause notice

10. Appeal against the competent authority

11. Review of the decision by the competent authority

12. Circulation of names of agencies with whom business dealings have been banned

1. Introduction

1.1 Central Bank of India, being a Public Sector Enterprise and 'State', within the meaning of Article 12 of Constitution of India, has to ensure preservation of rights enshrined in Chapter III of the Constitution. CENTRAL BANK OF INDIA has also to safeguard its commercial interests. CENTRAL BANK OF INDIA deals with Agencies, who have a very high degree of integrity, commitments and sincerity towards the work undertaken. It is not in the interest of CENTRAL BANK OF INDIA to deal with Agencies who commit deception, fraud or other misconduct in the execution of contracts awarded / orders issued to them. In order to ensure

compliance with the constitutional mandate, it is incumbent on CENTRAL BANK OF INDIA to observe principles of natural justice before banning the business dealings with any Agency.

1.2 Since banning of business dealings involves civil consequences for an Agency concerned, it is incumbent that adequate opportunity of hearing is provided and the explanation, if tendered, is considered before passing any order in this regard keeping in view the facts and circumstances of the case.

2. Scope

2.1 The General Conditions of Contract (GCC) of CENTRAL BANK OF INDIA generally

provide that CENTRAL BANK OF INDIA reserves its rights to remove from list of approved suppliers / contractors or to ban business dealings if any Agency has been found to have committed misconduct and also to suspend business dealings pending investigation. If such provision does not exist in any GCC, the same may be incorporated.

2.2 Similarly, in case of sale of material there is a clause to deal with the Agencies / customers

/ Buyers, who indulge in lifting of material in unauthorized manner. If such a stipulation does not exist in any Sale Order, the same may be incorporated.

2.3 However, absence of such a clause does not in any way restrict the right of Bank (CENTRAL BANK OF INDIA) to take action / decision under these guidelines in appropriate cases.

2.4 The procedure of (i) Removal of Agency from the List of approved suppliers / contractors; (ii) Suspension and (iii) Banning of Business Dealing with Agencies, has been laid down in these guidelines.

2.5 These guidelines apply to all the Units and subsidiaries of CENTRAL BANK OF INDIA.

2.6 It is clarified that these guidelines do not deal with the decision of the Management not to entertain any particular Agency due to its poor / inadequate performance or for any other reason.

2.7 The banning shall be with prospective effect, i.e., future business dealings.

3. Definitions

In these Guidelines, unless the context otherwise requires:

i) 'Party / Contractor / Supplier / Purchaser / Customer/Bidder/Tenderer' shall mean and include a public limited Bank or a private limited Bank, a firm whether registered or not, an individual, a cooperative society or an association or a group of persons engaged in any commerce, trade, industry, etc. 'Party / Contractor / Supplier / Purchaser / Customer/ Bidder / Tenderer' in the context of these guidelines is indicated as 'Agency'.

ii) 'Inter-connected Agency' shall mean two or more companies having any of the following features:

a) If one is a subsidiary of the other.

b) If the Director(s), Partner(s), Manager(s) or Representative(s) are common;

c) If management is common;

d) If one owns or controls the other in any manner;

iii) 'Competent Authority' and 'Appellate Authority' shall mean the following:

a) For Bank (entire CENTRAL BANK OF INDIA) wide Banning Executive Director (BSD) shall be the "Competent Authority" for the purpose of these guidelines. Chairman & Managing Director, CENTRAL BANK OF INDIA shall be the "Appellate Authority" in respect of such cases except banning of business dealings with Foreign Suppliers of imported coal/coke.

b) For banning of business dealings with Foreign Suppliers of imported goods, CENTRAL BANK OF INDIA Executive Directors" Committee (EDC) shall be the "Competent Authority". The Appeal against the Order passed by EDC, shall lie with Chairman & Managing Director, as First Appellate Authority.

c) In case the foreign supplier is not satisfied by the decision of the First Appellate Authority, it may approach CENTRAL BANK OF INDIA Board as Second Appellate Authority.

d) For Zonal Offices Only

Any officer not below the rank of Deputy General Manager appointed or nominated by the Head of Zonal Office shall be the "Competent Authority" for the purpose of these guidelines. The Head of the concerned Zonal Office shall be the "Appellate Authority" in all such cases.
e) For Corporate Office only

For procurement of items / award of contracts, to meet the requirement of Corporate Office only, Head of Business Support Department (BSD) shall be the "Competent Authority" and concerned Executive Director (BSD) shall be the "Appellate Authority".

e) Managing Director & CEO , CENTRAL BANK OF INDIA shall have overall power to take Suo-moto action on any information available or received by him and pass such order(s) as he may think appropriate, including modifying the order(s) passed by any authority under these guidelines.

iv) 'Investigating Department' shall mean any Department or Unit investigating into the conduct of the Agency and shall include the Vigilance Department, Central Bureau of Investigation, the State Police or any other department set up by the Central or State Government having powers to investigate.

v) 'List of approved Agencies - Parties / Contractors / Suppliers / Purchasers / Customers / Bidders / Tenderers shall mean and include list of approved / registered Agencies - Parties/ Contractors / Suppliers / Purchasers / Customers / Bidders / Tenderers, etc.

4. Initiation of Banning / Suspension

Action for banning / suspension business dealings with any Agency should be initiated by the department having business dealings with them after noticing the irregularities or misconduct on their part. Besides the concerned department, Vigilance Department of each Unit /Corporate Vigilance may also be competent to advise such action.

5. Suspension of Business Dealings

5.1 If the conduct of any Agency dealing with CENTRAL BANK OF INDIA is under investigation by any department (except Foreign Suppliers of imported goods), the Competent Authority may consider whether the allegations under investigation are of a serious nature and whether pending investigation, it would be advisable to continue business dealing with the Agency. If the Competent Authority, after consideration of the matter including the recommendation of the Investigating Department, if any, decides that it would not be in the interest to continue business dealings pending investigation, it may suspend business dealings with the Agency. The order to this effect may indicate a brief of the charges under investigation. If it is decided that inter-connected Agencies would also come within the ambit of the order of suspension, the same should be specifically stated in the order. The order of suspension would operate for a period not more than six months and may be communicated to the Agency as also to the Investigating Department. The Investigating Department may ensure that their investigation is completed and whole process of final order is over within such period.

5.2 The order of suspension shall be communicated to all Departmental Heads within the Plants / Units. During the period of suspension, no business dealing may be held with the Agency.

5.3 As far as possible, the existing contract(s) with the Agency may continue unless the Competent Authority, having regard to the circumstances of the case, decides otherwise.

5.4 If the gravity of the misconduct under investigation is very serious and it would not be in the interest of CENTRAL BANK OF INDIA, as a whole, to deal with such an Agency pending investigation, the Competent Authority may send his recommendation to ED (GAD), CENTRAL BANK OF INDIA Corporate Office along with the material available. If Corporate Office considers that depending upon the gravity of the misconduct, it would not be desirable for all the Units and Subsidiaries of CENTRAL BANK OF INDIA to have any dealings with the Agency concerned, an order suspending business dealings may be issued to all the Units by the Competent Authority of the Corporate Office, copy of which may be endorsed to the Agency concerned. Such an order would operate for a period of six months from the date of issue.

5.5 For suspension of business dealings with Foreign Suppliers of imported goods, following shall be the procedure:-

i) Suspension of the foreign suppliers shall apply throughout the Bank including Subsidiaries.
ii) Based on the complaint forwarded by ED (BSD) or received directly by Corporate Vigilance, if gravity of the misconduct under investigation is found serious and it is felt that it would not be in the interest of CENTRAL BANK OF INDIA to continue to deal with such agency, pending investigation, Corporate Vigilance may send such recommendation on the matter to Executive Director, BSD to place it before Executive Directors Committee (EDC) with ED (BSD) as Convener of the Committee. The committee shall expeditiously examine the report, give its comments/recommendations within twenty one days of receipt of the reference by ED, BSD.

iii) If EDC opines that it is a fit case for suspension, EDC may pass necessary orders which shall be communicated to the foreign supplier by ED, BSD.

5.6 If the Agency concerned asks for detailed reasons of suspension, the Agency may be informed that its conduct is under investigation. It is not necessary to enter into correspondence or argument with the Agency at this stage.

5.7 It is not necessary to give any show-cause notice or personal hearing to the Agency before issuing the order of suspension. However, if investigations are not complete in six months' time, the Competent Authority may extend the period of suspension by another three months, during which period the investigations must be completed.

6. Ground on which Banning of Business Dealings can be initiated

6.1 If the security consideration, including questions of loyalty of the Agency to the State, so warrant;

6.2 If the Director / Owner of the Agency, proprietor or partner of the firm, is convicted by a Court of Law for offences involving moral turpitude in relation to its business dealings with the Government or any other public sector enterprises or CENTRAL BANK OF INDIA, during the last five years;

6.3 If there is strong justification for believing that the Directors, Proprietors, Partners, owner of the Agency have been guilty of malpractices such as bribery, corruption, fraud, substitution of tenders, interpolations, etc.;

6.4 If the Agency continuously refuses to return / refund the dues of CENTRAL BANK OF INDIA without showing adequate reason and this is not due to any reasonable dispute which would attract proceedings in arbitration or Court of Law;

6.5 If the Agency employs a public servant dismissed / removed or employs a person convicted for an offence involving corruption or abetment of such offence;

6.6 If business dealings with the Agency have been banned by the Govt. or any other public sector enterprise;

6.7 If the Agency has resorted to Corrupt, fraudulent practices including misrepresentation of facts and / or fudging /forging /tampering of documents;

6.8 If the Agency uses intimidation / threatening or brings undue outside pressure on the Bank (CENTRAL BANK OF INDIA) or its official in acceptance / performances of the job under the contract;

6.9 If the Agency indulges in repeated and / or deliberate use of delay tactics in complying with contractual stipulations;

6.10 Wilful indulgence by the Agency in supplying sub-standard material irrespective of whether pre-dispatch inspection was carried out by Bank (CENTRAL BANK OF INDIA) or not;

6.11 Based on the findings of the investigation report of CBI / Police against the Agency for mala fide / unlawful acts or improper conduct on his part in matters relating to the Bank

(CENTRAL BANK OF INDIA) or even otherwise;

6.12 Established litigant nature of the Agency to derive undue benefit;

6.13 Continued poor performance of the Agency in several contracts;

6.14 If the Agency misuses the premises or facilities of the Bank (CENTRAL BANK OF INDIA), forcefully occupies, tampers or damages the Bank's properties including land, water resources, forests / trees, etc.

(Note: The examples given above are only illustrative and not exhaustive. The Competent

Authority may decide to ban business dealing for any good and sufficient reason).

7 Banning of Business Dealings

7.1 A decision to ban business dealings with any Agency should apply throughout the Bank

Including Subsidiaries.

7.2 There will be a Standing Committee in each Zone to be appointed by Head of Zonal Office for processing the cases of "Banning of Business Dealings" except for banning of business dealings with foreign suppliers of goods. However, for procurement of items / award of contracts, to meet the requirement of Corporate Office only, the committee shall be consisting of General Manager / Dy. General Manager each from Operations, Law & BSD. Member from BSD shall be the convener of the committee. The functions of the committee shall, inter-alia include:

i) To study the report of the Investigating Agency and decide if a prima-facie case for Bank-wide / Local unit wise banning exists, if not, send back the case to the Competent Authority. ii) To recommend for issue of show-cause notice to the Agency by the concerned department. iii) To examine the reply to show-cause notice and call the Agency for personal hearing, if required.

iv)To submit final recommendation to the Competent Authority for banning or otherwise.

7.3 If Bank wide banning is contemplated by the banning Committee of any Zone, the proposal should be sent by the committee to ED (BSD) through the Head of the Zonal Office setting out the facts of the case and the justification of the action proposed along with all the relevant papers and documents. GAD shall get feedback about that agency from all other Zones and based on this feedback, a prima-facie decision for banning / or otherwise shall be taken by the Competent Authority. At this stage if it is felt by the Competent Authority that there is no sufficient ground for Bank wide banning, then the case shall be sent back to the Head of Zonal Office for further action at the Zone level. If the prima-facie decision for Bank-wide banning has been taken, ED (BSD) shall issue a show-cause notice to the agency conveying why it should not be banned throughout CENTRAL BANK OF INDIA.

After considering the reply of the Agency and other circumstances and facts of the case, ED (BSD) will submit the case to the Competent Authority to take a final decision for Bank-wide banning or otherwise.

7.4 If the Competent Authority is prima-facie of view that action for banning business dealings with the Agency is called for, a show-cause notice may be issued to the Agency as per paragraph 9.1 and an enquiry held accordingly.

7.5 Procedure for Banning of Business Dealings with Foreign Suppliers of imported goods.

• Banning of the agencies shall apply throughout the Bank including Subsidiaries.

• Based on the complaint forwarded by ED (BSD) or received directly by Corporate Vigilance, if gravity of the misconduct under investigation is found serious and it is felt that it would not be in the interest of CENTRAL BANK OF INDIA to continue to deal with such agency, pending investigation, Corporate Vigilance may send such recommendation on the matter to Executive Director, BSD to place it before Executive Directors" Committee (EDC) with ED (BSD) as Convener of the Committee.

• The committee shall expeditiously examine the report, give its comments/recommendations within twenty one days of receipt of the reference by ED, BSD.

• If EDC opines that it is a fit case for initiating banning action, it will direct ED (BSD) to issue show-cause notice to the agency for replying within a reasonable period.

• On receipt of the reply or on expiry of the stipulated period, the case shall be submitted by ED (BSD) to EDC for consideration & decision.

• The decision of the EDC shall be communicated to the agency by ED (BSD).

8 Removal from List of Approved Agencies - Suppliers / Contractors, etc.

8.1 If the Competent Authority decides that the charge against the Agency is of a minor nature,

it may issue a show-cause notice as to why the name of the Agency should not be removed from the list of approved Agencies - Suppliers / Contractors, etc.

8.2 The effect of such an order would be that the Agency would not be disqualified from Competing in Open Tender Enquiries but Limited Tender Enquiry (LTE) may not be given to the Agency concerned.

8.3 Past performance of the Agency may be taken into account while processing for approval of the Competent Authority for awarding the contract.

9 Show Cause Notice

9.1 In case where the Competent Authority decides that action against an Agency is called for, a show-cause notice has to be issued to the Agency. Statement containing the imputation of misconduct or misbehaviour may be appended to the show-cause notice and the Agency should be asked to submit within 15 days a written statement in its defence.

9.2 If the Agency requests for inspection of any relevant document in possession of CENTRAL BANK OF INDIA, necessary facility for inspection of documents may be provided.

9.3 The Competent Authority may consider and pass an appropriate speaking order:

a) For exonerating the Agency if the charges are not established;

b) For removing the Agency from the list of approved Suppliers / Contactors, etc. c) For banning the business dealing with the Agency.

9.4 If it decides to ban business dealings, the period for which the ban would be operative may be mentioned. The order may also mention that the ban would extend to the interconnected Agencies of the Agency.

10 Appeal against the Decision of the Competent Authority

10.1 The Agency may file an appeal against the order of the Competent Authority banning business dealing, etc. The appeal shall lie to Appellate Authority. Such an appeal shall be preferred within one month from the date of receipt of the order banning business dealing, etc.

10.2 Appellate Authority would consider the appeal and pass appropriate order which shall be communicated to the Agency as well as the Competent Authority.

11 Review of the Decision by the Competent Authority

Any petition / application filed by the Agency concerning the review of the banning order passed originally by Competent Authority under the existing guidelines either before or after filing of appeal before the Appellate Authority or after disposal of appeal by the Appellate Authority, the review petition can be decided by the Competent Authority upon disclosure of

new facts / circumstances or subsequent development necessitating such review. The Competent Authority may refer the same petition to the Standing Committee/EDC as the case may be for examination and recommendation.

12 Circulation of the names of Agencies with whom Business Dealings have been banned

12.1 Depending upon the gravity of misconduct established, the Competent Authority of the

Corporate Office may circulate the names of Agency with whom business dealings have been banned, to the Government Departments, other Public Sector Enterprises, etc. for such action as they deem appropriate.

12.2 If Government Departments or a Public Sector Enterprise request for more information about the Agency with whom business dealings have been banned, a copy of the report of Inquiring Authority together with a copy of the order of the Competent Authority / Appellate Authority may be supplied.

12.3 If business dealings with any Agency has been banned by the Central or State Government or any other Public Sector Enterprise, CENTRAL BANK OF INDIA may, without any further enquiry or investigation, issue an order banning business dealing with the Agency and its inter-connected Agencies.

12.4 Based on the above, Zonal Offices may formulate their own procedure for implementation of the Guidelines and same be made a part of the tender documents

83. ANNEXURE 19: UNDERTAKING FOR 2 YEARS ROADMAP

(This undertaking should be on the letterhead of the bidder duly signed by an authorized signatory)

Date :
To,
CISO,
Central Bank Of India,
Information Security Department,
Plot no-26, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,
Sub: RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank

Tender No. GEM/2026/B/8006355

We, _____ hereby confirm that as a bidder and the service provider, would provide Cyber Security Consultancy for various consultancy services and activities related to Information Technology and Cyber Security Services to the Bank along with Facility Management Services. We also commit to support the proposed Solutions for a minimum period of 2 years.

Yours faithfully,

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

Date:
Place:

84. Annexure 20: Undertaking For Information Security

(This undertaking should be on the letterhead of the bidder duly signed by an authorized signatory)

Date :
To,
CISO,
Central Bank Of India,
Information Security Department,
Plot no-26, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,
Sub: RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank

Tender No. GEM/2026/B/8006355

We hereby undertake that the proposed solution / software to be supplied will be free of malware, free of any obvious bugs and free of any covert channels in the code (of the version of the application being delivered as well as any subsequent versions/ modifications done).

Also, undertake that the proposed solution / software to be supplied will be complying to Bank's Information Security Policy (of the version of the application being delivered as well as any subsequent versions/modifications done). And new Information Security requirement will be compiled within the timeline set by Bank / Regulatory agencies.

Yours faithfully,

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

Date:
Place:

85. ANNEXURE 21: UNDERTAKING FOR AUTHENTICITY OF THE PRODUCT

(This undertaking should be on the letterhead of the bidder duly signed by an authorized signatory)

Date :
To,
CISO,
Central Bank Of India,
Information Security Department,
Plot no-26, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,
Sub: RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank

Tender No. GEM/2026/B/8006355

With reference to RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank.

We hereby undertake to produce the certificate from our OEM supplier in support of this undertaking at the time of delivery/installation. It will be our responsibility to produce such letters from our OEM suppliers at the time of delivery or within a reasonable time.

In case of default and we are unable to comply with the above at any time, we agree to take back the Licenses without demur, if already supplied and return the money if any paid to us by you in this regard.

Yours faithfully,

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

Date:
Place:

86. ANNEXURE 22: LIST OF SOFTWARE AND HARDWARE COMPONENTS REQUIRED FOR IMPLEMENTATION

(This undertaking should be on the letterhead of the bidder duly signed by an authorized signatory)

Date :
To,
CISO,
Central Bank Of India,
Information Security Department,
Plot no-26, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,
Sub: RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank

Tender No. GEM/2026/B/8006355

With reference to RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank

The below software are proposed for implementation of scope mentioned in RFP. If Bank would like to procure the below licenses (Complete or partial) independently, we will support and co-operate with Bank for procurement of licenses in line with CVC guidelines.

Sr. No.	Software / Tool or Component Required	OEM Name	Justification (Why Software is needed)	Licensing Metric for software (User Based/ Processor Based/ any other)

The below Hardware items are proposed for implementation of scope mentioned in RFP. If Bank would like to procure the below items (Complete or partial) independently, we will support and co-operate with Bank for procurement of licenses in line with CVC guidelines

Sr. No.	Hardware Item or	Quantity	OEM Name	Size of Hardware for provisioning Racks space	Number of Power Inputs and Power

	Component Required				consumption for device

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

87. ANNEXURE 23: PROPOSED TEAM PROFILE

(This undertaking should be on the letterhead of the bidder duly signed by an authorized signatory)

Date :
To,
CISO,
Central Bank Of India,
Information Security Department,
Plot no-26, Sector-11,
CBD Belapur, Navi Mumbai- 400614

Sir,
Sub: RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank

Tender No. GEM/2026/B/8006355

RFP for Appointment of Consultant for Consultancy and Implementation activities related with IT and Cyber Security Services to the Bank

S. No.	TYPE OF WORK	NAME OF TEAM MEMBERS	QUALIFICATION & CERTIFICATION	PREVIOUS BANKS WHERE TEAM MEMBER WAS ASSOCIATED	DURATION OF TEAM MEMBER ASSOCIATION	NO. OF YEARS OF EXPERIENCE

We hereby acknowledge that the information provided by us is true and to the Best of our Knowledge
Date:
Place:
Signature of Authorized Signatory:
Name of Signatory:
Designation:
Seal of Company: