

PUNJAB & SIND BANK



**REQUEST FOR PROPOSAL
FOR
SELECTION OF BIDDER FOR SUPPLY INSTALLATION, IMPLEMENTATION,
MAINTENANCE & MANAGEMENT OF IT SECURITY SOLUTION & SERVICES**

RFP No. PSB/HOIT/RFP/53/2026-27

dated 19.08.2026

**HEAD OFFICE IT DEPARTMENT
2ND FLOOR,
PLOT NO. 151, SECTOR 44
INSTITUTIONAL AREA, GURUGRAM -122003**

1	KEY INFORMATION.....	7
2	GLOSSARY	10
3	DISCLAIMER.....	14
4	INTRODUCTION	15
5	PROJECT OBJECTIVE.....	15
6	INSTRUCTION TO BIDDER	16
6.1	Language of the Bid	16
6.2	Bid Currency & Price Structure	16
6.3	Bid System Offer	16
6.4	Two Bid System:	16
6.4.1	Preparation of Bids:	17
6.5	Cost of Preparation	19
6.6	Normalization of Bids	19
6.7	Submission of Bid and communication	20
6.8	Late bids	20
6.9	Modifications and/ or Withdrawal of Bids	21
6.10	Earnest Money Deposit (EMD):.....	21
6.11	Performance Bank Guarantee/Security Deposit (PBG)	22
6.12	No commitment to accept lowest or any bid	23
6.13	Right To Accept Any Bid and To Reject Any OR All Bids/Cancellation of Tender process...23	
6.14	Correction of Errors	23
6.15	Soft copy of tender document	24
6.16	Bid validity period	25
6.17	Pre-bid meeting	25
6.18	Amendment to RFP Contents	26
6.19	Disqualification	26
6.20	Fixed Price.....	26
6.21	Project Execution	26
6.22	Confidentiality of the Bid Document	26
7	SCOPE OF WORK	27
7.1	IT Security Solution & Services	28

7.2	RACI (Responsible, Accountable, Consulted, Informed)	33
7.3	Functional Requirements	34
7.3.1	Perimeter & Network Security	34
7.3.2	End Point Security	40
7.3.3	Data Security	42
7.3.4	Application Security	43
7.3.5	Management Layer Security	47
7.4	Bidder Responsibilities	50
7.5	OEM Responsibilities	51
7.5.1	Migration - Activities are to be performed by Respective solution OEM (supported by bidder) 52	
7.5.2	Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder)	55
7.5.3	System Design - Activities are to be performed by Respective solution OEM (supported by bidder)	56
7.5.4	Development and Installation - Activities are to be performed by Respective Solution OEM (supported by bidder)	57
7.5.5	Documentation - Activities are to be performed by Respective solution OEM (supported by bidder)	58
7.5.6	Deployment and Go-Live - Activities are to be performed by Respective Solution OEM (supported by bidder)	58
7.5.7	Testing- Activities are to be performed by Respective solution OEM (supported by bidder) 59	
7.5.8	Training- Activities are to be performed by Respective solution OEM (supported by bidder) 61	
7.5.9	Security requirements - Activities are to be performed by Respective solution OEM (supported by bidder)	62
7.6	Cloud Service Provider Responsibilities	63
7.7	Non-functional requirements	66
7.8	Delivery, Installation & Commissioning	66
7.9	Data Privacy	67
7.10	Solution/Appliance Warranty, ATS and AMC	69
7.11	Resource Requirement	70
7.12	Facilities Management	76
7.12.1	Continual Improvement	79
7.12.2	DR Drill	82

7.12.3	IT Security operations	82
7.12.4	OEM Services & Deployment (Architecture Assessment):	86
7.12.5	System recovery	87
7.13	IT Infrastructure	88
7.14	Other In-Scope services	93
7.14.1	Other Scope Activity	93
7.14.2	Transition Management	94
7.14.3	Security Management	95
7.14.4	DR Setup - Activities are to be performed by Respective Solution OEM (supported by bidder) 96	
8	CONTRACT PERIOD	97
9	PROJECT TIMELINES	97
10	EVALUATION CRITERIA	98
10.1	Preliminary Scrutiny	98
10.2	Eligibility Evaluation Criteria	100
10.3	Technical Evaluation Criteria	111
10.4	Commercial Evaluation Criteria	114
11	PAYMENT TERMS	115
11.1	Product (Software) Cost	116
11.2	OEM Services Cost	117
11.3	Hardware Cost	117
11.4	ATS/subscription cost & AMC Cost	118
11.5	Facility Management (FM) Cost:	118
11.6	Other Cost	118
12	SERVICE LEVELS & PENALTIES	119
12.1	Service Level Agreement	119
12.2	Penalties	135
12.3	At-Risk Amount	135
13	TERMS AND CONDITIONS	136
13.1	Assignment & Subcontracting	136
13.2	Right to Alter quantities	136
13.3	Delays in the Bidder's Performance	136
13.4	Jurisdiction	136
13.5	Dispute Resolution	137

13.6	Notices	137
13.7	Legal Compliance	138
13.8	Digital Personal Data Protection Compliance	138
13.9	Non-Disclosure Agreement	138
13.10	Solicitation of Employees	139
13.11	Authorized Signatory.....	139
13.12	Confidentiality.....	139
13.13	Indemnity.....	140
13.14	Make in India	140
13.15	Force Majeure	141
13.16	Ownership & Retention of Documents:.....	141
13.17	Conflict of Interest:	142
13.18	Signing of Pre-Contract Integrity Pact:	142
13.19	Liquidated Damages.....	142
13.20	Intellectual Property Indemnity:.....	143
13.21	Limitation of Liability	143
13.22	Order Cancellation	144
13.23	Consequences of Termination.....	145
13.24	Audit by Third Party.....	146
13.25	Access Through Virtual Private Network (VPN).....	147
13.26	INSURANCE.....	148
13.27	SEVERABILITY	148
13.28	NO LIEN OVER BANK DATA	148
14	APPENDIX	149
14.1	APPENDIX 1A: Functional Compliance Sheet:	149
14.2	APPENDIX 1B: Technical Compliance Sheet:	149
14.3	APPENDIX 2: Commercial Bill of material Sheet.....	149
14.4	APPENDIX 3: IT Infrastructure Virtual To Physical (V2P) Mapping	149
15	ANNEXURES.....	150
15.1	Annexure 1: Submission Checklist (on bidder's letterhead)	150
15.2	Annexure 2: Bidder's Information.....	151
15.3	Annexure 3: Tender Covering Letter	154
15.4	Annexure 4: Bid Security Declaration.....	156
15.5	Annexure 5: Pre-Qualification Criteria.....	158

15.6	Annexure 6: Acceptance/Compliance Certificate	170
15.7	Annexure 7: Minimum Local Content Certification	171
15.8	Annexure 8: Certification on OEM Requirements	172
15.9	Annexure 9: Escalation Matrix	174
15.10	Annexure 10: Litigation Certificate	175
15.11	Annexure 11: Non-blacklisting undertaking	176
15.12	Annexure 12: Undertaking of Authenticity (on bidder's letterhead)	177
15.13	Annexure 13: Non-Disclosure Agreement	179
15.14	Annexure 14: Commercial Proposal Submission Checklist	185
15.15	Annexure 15: Bank Guarantee Format for Earnest Money Deposit	186
15.16	Annexure 16: Format of Performance Guarantee	188
15.17	Annexure 17 : Pre-contract integrity pact	191
15.18	Annexure 18: Compliance with FRS, TRS, SoW & SBOM (on respective OEM letterhead) 197	
15.19	Annexure 19: Stack Confirmation Sheet- Undertaking for Proposed OEM Products	199
15.20	Annexure 20: S-BOM & C-BOM DETAILS of all the proposed Tool/solutions	201
15.21	Annexure 21: Sizing/Volumetrics, Data Retention and Current Infrastructure	203
15.21.1	Existing and Envisaged Stack:	203
15.21.2	Existing IT Security Solution Details	205
15.21.3	Current IT assets	206
15.21.4	Deployment & Data Retention	207
15.22	Annexure 22: Client References Format	214
15.23	Annexure 23: Pre-bid Query format	217
15.24	Annexure 24: Proposed Resources CV	218
15.25	Annexure 25: Insurance Surety Bond against EMD	219

1 KEY INFORMATION

Particulars	Details
Tender Title	Selection of Bidder for Supply Installation, Implementation, Maintenance & Management of IT Security Solutions & Services
Security Deposit/Earnest Money deposit	Rs. 8.65 Cr (INR Eight crore sixty five lakh only) Note: - Bidders who are eligible for EMD (Earnest Money Deposit) exemption as per latest GeM General Terms and Conditions are required to submit a Bid Security Declaration in lieu of EMD. Please refer to RFP, Annexure 4: Bid Security Declaration for the prescribed format. This declaration must be duly filled, signed, and submitted along with the bid documents by vendors seeking the waiver of EMD submission. Failure to submit the Bid Security Declaration (where applicable) will result in the bid being treated as non-responsive.
Bid validity	180 days from the date of opening of the bid.
Performance Bank Guarantee	5% of Project Cost The selected bidder shall be responsible for providing the PBG for the duration of the contract (Including the extension) + claim period (12 months) of the Bank guarantees
Date of Publishing the tender on Bank's Website	19 th August 2026
Last Date for submission of Pre-Bid Query	26th August 2026 a) Pre bid queries should be submitted as per Annexure 23 in MS- excel format. b) Queries should be submitted through GEM c) Queries must also be mailed to bank (queries must be mailed to hoit.tenders@psb.bank.in only) quoting tender reference number in the subject. Subject of the email should be given as "Pre-Bid Queries for Selection of Bidder for Supply Installation, Implementation, Maintenance & Management of IT Security Solutions & Services. d) Queries arriving afterwards will not be entertained/responded.
Date and Time for Pre-Bid Meeting	27th August 2026, 11am - Pre-Bid meeting will be held online, and participants are requested to attend the meeting through the link shared by the bank. - A maximum of two (2) representatives from each bidder shall be permitted to attend the pre-bid meeting. The representatives must be

Particulars	Details
	duly authorized by the bidder through an authorization letter. The authorization letter shall be submitted through an email along with the pre-bid queries. - Those who are interested in participating the Prebid meeting should share the participant details to hoit.tenders@psb.bank.in. - Link of the pre-bid meeting will be shared with participants having the authorization for whom the authorization letter has been shared Upon perusal of the same, the link / meeting id will be shared to the participant to participate in the virtual meeting.
Last Date and Time for submission of Bids	16 th September 2026, 3pm
Date and Time of Opening of Bids	16 th September 2026, 3:30pm
Date and Time of online Commercial Bids	To be notified later to the qualifying bidders only.
Place of Opening of Bids	Punjab & Sind Bank Head Office: HO IT, 2nd Floor, Plot No. 151, Sector 44, Institutional Area, Gurugram -122003.
Contact Persons for any clarifications/ Submission of Bids	- Name: Mr. Pranay Shankar Thakur – CM (IT) Email Id: pranay.thakur@psb.bank.in Mobile: +91 8750661322 - Name: Mr. Nitin Kumar (Manager – IT) Email Id: nitin.kumar3@psb.bank.in Mobile: +91 9082688275
Project Office Location	Punjab & Sind Bank Head Office: HO IT, 2nd Floor, Plot No. 151, Sector 44, Institutional Area, Gurugram -122003.
	- No suggestions or queries shall be entertained after pre-bid meeting. - This document can be downloaded from following website: https://punjabandsind.bank.in .Any Amendments, Modifications, Pre-Bid Replies, Clarifications & any communication etc. will be uploaded on the Bank's website (i.e. https://punjabandsind.bank.in & https://gem.gov.in/ - No individual communication will be sent to the individual bidders.
Information for Online Participating: The following activities will be conducted online through the https://gem.gov.in/ website: - Purchase of RFP document including all Annexures. - Addendums to the RFP.	

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

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

Note:

1. If any of the dates given above happens to be Holiday in Banks in Haryana, the related activity shall be undertaken on the next working day at the same time.
2. All Claims made by the Bidder will have to be backed by documentary evidence.
3. Bidders should submit bids well before time rather than wait for the last moment to avoid any technical glitches or networking issues etc. at their end.
4. Bidders are requested to use a reliable internet connection (data cable / broadband) to safeguard themselves. The bank is not responsible for telephone line glitches, internet response issues, hardware hangs etc. at bidder's end.
5. No Claim of any bidder shall be entertained, whatsoever for delayed submission of their bid at any stage because of any reason. Therefore, bidders are advised to submit their bids well before the scheduled time.

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

2 GLOSSARY

Acronym	Abbreviation
AMC	Annual Maintenance Contract
APT	Advanced Persistent Threat
ATS	Annual Technical Support
BFSI	Banking, Financial Services, and Insurance
CBOM	Cryptographic Bill of Material
CCIL	Clearing Corporation of India Ltd
CEH	Certified Ethical Hacker
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CISM	Certified Information Security Manager
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CK	Cyber Kill Chain
CPU	Central Processing Unit
CVE	Common Vulnerabilities and Exposures
DAM	Database Activity Monitoring
DB	Database
DC	Data Center
DDoS	Distributed Denial of Service
DFP	Data Flow Protection
DIC	District Industries Centre
DIPP	Department for Promotion of Industry and Internal Trade
DKIM	DomainKeys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting & Conformance
DNS	Domain Name System
DPDP	Digital Personal Data Protection Act
DR	Disaster Recovery
DRC	Disaster Recovery Center
DSS	Data Security Standard
EMD	Earnest Money Deposit
FC	Fibre Channel
FM	Facilities Management
FRD	Functional Requirements Document
FRSM	Functional Requirements Specification Matrix
FTP	File Transfer Protocol
GCIA	GIAC Certified Intrusion Analyst
GDPR	General Data Protection Regulation

Acronym	Abbreviation
GOI	Government of India
GST	Goods and Services Tax
GUI	Graphical User Interface
HA	High Availability
HIPS	Host-based Intrusion Prevention System
HIPAA	Health Insurance Portability and Accountability Act
HLD	High-Level Design
HO	Head Office
IDR	Identity Detection and Response
INR	Indian Rupee
IOPS	Input/Output Operations Per Second
ISO	International Organization for Standardization
IT	Information Technology
ITSM	IT Service Management
KVIB	Khadi and Village Industries Board
KVIC	Khadi and Village Industries Commission
LAN	Local Area Network
LD	Liquidated Damages
LDAP	Lightweight Directory Access Protocol
LLD	Low-Level Design
LOI	Letter of Intent
MIS	Management Information System
MTBF	Mean Time Between Failures
MTTD	Mean Time to Detect
MTTR	Mean Time to Resolve/Repair
NAC	Network Access Control
NAT	Network Address Translation
NCIIPC	National Critical Information Infrastructure Protection Centre
NDA	Non-Disclosure Agreement
NDR	Network Detection and Response
NEFT	National Electronic Funds Transfer
NGFW	Next Generation Firewall
NIST	National Institute of Standards and Technology
NPCI	National Payments Corporation of India
NSIC	National Small Industries Corporation
NSPM	Network Security Policy Management
OD	Overdraft
OEM	Original Equipment Manufacturer
OM	Operations Manual / Order Management
OS	Operating System

Acronym	Abbreviation
OWASP	Open Web Application Security Project
PAM	Privileged Access Management
PAN	Permanent Account Number
PBG	Performance Bank Guarantee
PCAP	Packet Capture
PIM	Privileged Identity Management
PSU	Public Sector Undertaking
RACI	Responsible, Accountable, Consulted, Informed
RBI	Reserve Bank of India
RCA	Root Cause Analysis
RDBMS	Relational Database Management System
RDP	Remote Desktop Protocol
RFP	Request for Proposal
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAN	Storage Area Network
SANS	SysAdmin, Audit, Network, and Security Institute
SBOM	Software Bill of Materials
SCD	Software Configuration Document
SFG	Secure File Gateway
SFMS	Structured Financial Messaging System
SFTP	Secure File Transfer Protocol
SIEM	Security Information and Event Management
SIT	System Integration Testing
SLA	Service Level Agreement
SOAP	Simple Object Access Protocol
SOC	Security Operations Center
SOD	Segregation of Duties
SPOC	Single Point of Contact
SRS	Software Requirements Specification
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	System Testing
TCP	Transmission Control Protocol
TDS	Tax Deducted at Source
UAT	User Acceptance Testing
UDP	User Datagram Protocol
UEM	Unified Endpoint Management
UNIX	Uniplexed Information and Computing System
USB	Universal Serial Bus

Acronym	Abbreviation
VAPT	Vulnerability Assessment and Penetration Testing
VPC	Virtual Private Cloud
VPN	Virtual Private Network
WAF	Web Application Firewall
XDR	Extended Detection and Response
XML	Extensible Markup Language
ZTA	Zero Trust Architecture
ZTNA	Zero Trust Network Access

3 DISCLAIMER

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

4 INTRODUCTION

Punjab & Sind Bank (hereon referred to as ‘PSB’ or the ‘Bank’) is a major Public Sector bank in Northern India. The Bank's Corporate Office is in Kidwai Nagar, New Delhi. The Bank has a national presence through a widespread network of 1657 branches all networked under Centralized banking Solution on Finacle. It also has a network of more than 1175 ATM(s) spread across the country including onsite and offsite ATMs as well. With more than 119 years of customer services, the Bank has a large, satisfied clientele throughout the country. For enhancing customer convenience levels and overall inter-branch efficiency, the bank has been a front runner in implementing various IT-enabled products. Bank has already launched various delivery channels such as Internet Banking, Mobile Banking, and ATMs. Bank has migrated its Core Banking platform to Finacle 10 version. Also, bank has deployed IT solutions like NAC solution, Secure web gateway/web proxy solution, Patch Management Solution, IT Inventory Management, Application Whitelisting, Mobile Device Management (MDM) solution, SDWAN, SDN, ITSM, Change management, Incident management etc. The Bank invites Request for Proposal for Selection of Bidder for Supply Installation, Implementation, Maintenance & Management of IT Security Solutions & Services

5 PROJECT OBJECTIVE

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

This RFP invites technically mature, scalable, and interoperable solutions from eligible bidders to enable the Bank to establish a multi-layered security architecture covering perimeter security, network security, and related cybersecurity domains.

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

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

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

The methodology for submission of bids is detailed in Section 6: Instructions to Bidders. The Terms and Conditions of Contract (TCC) are provided in Section 13 of this RFP.

This Request for Proposal (RFP) has been prepared solely for the purpose of enabling Punjab & Sind Bank (hereinafter referred to as “the Bank”) to select a bidder for the supply, installation, implementation, maintenance, and management of IT Security Solutions & Services

6 INSTRUCTION TO BIDDER

6.1 Language of the Bid

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

6.2 Bid Currency & Price Structure

Prices shall be expressed in the Indian Rupees only. The bidder must quote price exclusive of all applicable GST. The cost will not depend on any variation in the dollar exchange rate/change in tax structure.

6.3 Bid System Offer

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

6.4 Two Bid System:

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

Part A- Technical cum Eligibility Proposal: Indicating the response to the Pre-Qualification Criteria, Technical evaluation criteria, Appendix & annexures for Technical and Eligibility requirement,

Compliance to Scope of Work and other terms & conditions. The format for submission of Technical Proposal is as per Annexure 1: Submission checklist along with Appendix 1: Functional Specification Sheet, Appendix 1B: Technical specification sheet, Appendix 3: Virtual to physical mapping, and Appendix 2: Masked Bill of Material.

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

6.4.1 Preparation of Bids:

6.4.1.1 Part A – Technical cum Eligibility Proposal

1. Before submitting the bid, the bidders should ensure that they have reviewed the terms and conform to the Pre-Qualification Criteria as stated in RFP. Only after satisfying themselves of the Pre-Qualification Criteria, the Offer should be submitted.
2. Technical cum eligibility Proposal should be submitted as per the format in Annexure 1: Submission Checklist. Relevant technical details and documentation should be provided along with Technical Proposal.
3. It is mandatory to provide compliance with the scope, requirements, and terms required by the bank.
4. The offer may not be evaluated and may be rejected by the Bank without any further reference in case of non-adherence to the format or partial submission of information as per the format given in the proposal and not in conformity to the RFP requirement.
5. No modification, alteration, or deviation from the technical and functional requirements proposed by the bidder shall be permitted after submission of the Bid. The submitted proposal shall be treated as final and binding.
6. Bidders shall submit complete details of the proposed solution, including product information, make/brand, model details, product brochures, technical datasheets, functional specifications, and all other relevant supporting documentation along with the Bid. Failure to submit this information along with the offer may result in disqualification.
7. The Technical Proposal shall be complete in all respects and shall contain all information sought under this RFP.
8. A Masked Bill of Material (BoM) must be submitted as part of the Technical Proposal and shall not contain any commercial or pricing information whatsoever.
 - a) The Masked BoM shall cover all products, licenses, hardware, software, subscriptions, services, implementation components, and support services proposed under the solution.
 - b) The Masked BoM shall be an exact replica of the Commercial Bill of Material in terms of item descriptions, quantities, specifications, part numbers, and solution components, with the sole exception that all pricing-related information shall be completely masked or removed.
 - c) The **Masked BoM shall not contain any commercial information** including, but not limited to, unit prices, extended prices, taxes, duties, GST percentages, tax amounts, discounts, commercial values, or any other pricing-related details.

- d) Technical Proposals submitted without a Masked BoM, or with a Masked BoM that does not comply with the instructions specified in this RFP, shall be liable for rejection at the sole discretion of the Bank.

6.4.1.2 Part B - Commercial Bid

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

NOTE:

1. All declarations, claims, certifications, compliances, experience credentials, technical specifications, and other representations made by the bidder in its Bid shall be supported by appropriate documentary evidence and submitted as part of the Bid. The Bank reserves the right to verify any information, document, or claim furnished by the bidder at any stage of the procurement process.
2. Bidders are advised to carefully examine and fully understand all instructions, eligibility requirements, formats, terms and conditions, scope of work, technical specifications, and other requirements contained in this RFP prior to submission of their Bid.

3. Failure to furnish all information, documents, clarifications, and supporting evidence required under the RFP, or submission of a Bid that is incomplete, inaccurate, misleading, conditional, or not substantially responsive to the requirements of the RFP, shall be solely at the bidder's risk and responsibility and may result in rejection of the Bid without any further reference to the bidder.
4. The Bank shall not be responsible for any omission, misunderstanding, or misinterpretation of the provisions of the RFP by the bidder.

6.5 Cost of Preparation

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

6.6 Normalization of Bids

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

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

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

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

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

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

The Bidders agree that they have no reservation or objection to the normalization process, defined methodology, and all the technically short-listed Bidders will, by responding to this RFP, agree to

participate in the normalization process and extend their co-operation to the Bank during this process. The Bidders, by submitting the response to this RFP, agree to the process and conditions of the normalization process.

6.7 Submission of Bid and communication

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

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

1. The Technical Bid shall be submitted online through the GeM Portal, however the EMD and IP needs to be submitted within 48 hours in hard copy.

2. Commercial Bid – Only Online (on GEM Portal)

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

General Manager

Punjab & Sind Bank

Second Floor

IT Department

Plot Number 151, Sector 44, Gurugram, 122003

E-mail: hoit.tenders@psb.bank.in

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

Bank reserves its right to cancel the order even after issuing the letter of Intent (LOI) / Purchase Order, if bank receives any directions / orders from Statutory Body / RBI/Govt. of India in a nature that binds the bank not to take the project forward or any reasons whatsoever. The decision of the Bank shall be final in this regard without disclosing any reason to any bidder or person.

6.8 Late bids

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

4. The Bidder must submit the bid as specified in Section 1: Key Information, bank has all the right to disqualify the bidder.

6.9 Modifications and/ or Withdrawal of Bids

1. Bids once submitted will be treated as final and no modification will be permitted. No Correspondence in this regard will be entertained.
2. The Bid should contain no alterations, erasures, or overwriting. The Bidder is expected to examine all instructions, forms, terms and specifications in the bidding documents. Failure to furnish all information required by the bidding documents or submission of bid not substantially / conclusively responsive to the bidding documents in every respect will be at the Bidders risk and may result in rejection of the bid.
3. No bidder shall be allowed to withdraw the bid after the deadline for submission of bids.
4. In the case of the successful bidder, he will not be allowed to withdraw/back out from the bid commitments. The bid earnest money in such eventuality shall be forfeited and all interests/claims of such bidder shall be deemed as foreclosed

6.10 Earnest Money Deposit (EMD):

1. The bidder shall furnish Noninterest earning Earnest Money Deposit (EMD) amount as mentioned in the Bid Schedule by way of Bank Guarantee drawn on any Scheduled Bank in India (except Cooperative Bank, RRB & Punjab & Sind Bank) in favor of Punjab & Sind Bank, payable at Delhi (format prescribed in Annexure 15: Bank Guarantee Format for Earnest Money Deposit) or Insurance Surety Bond (format prescribed in Annexure 25: Insurance Surety Bond against EMD)
2. EMD in the form of bank guarantee
 - a) The Bank Guarantee should be valid for an additional 45 days beyond bid validity period. Bank at its discretion can demand for extension for the validity of EMD. The format for submission of EMD in the form of Bank Guarantee is as per Annexure 15.
 - b) The Bank Guarantee issued by the issuing Bank on behalf of Bidder in favor of Bank shall be in paper form as well as issued under the "Structured Financial Messaging System" (SFMS) sent to Punjab & Sind Bank, Sector 44 Branch, Gurgaon, IFSC PSIB0021509. Any bank guarantee submitted in physical mode, including EMD/bid guarantee which cannot be verifiable through SFMS will be rejected summarily.
3. Non submission of EMD leads to rejection of Bid.
4. All MSEs having registration as per provisions of the Public Procurement Policy for Micro and Small Enterprises i.e. District Industries Centre (DIC) or Khadi and Village Industries Commission (KVIC) or Khadi and Industries Board (KVIB) or Coir Board or National Small Industries Commission (NSIC) or directorate of Handicrafts and Handlooms or Udyog Aadhaar Memorandum or any other body specified by Ministry of MSME and Start-ups (recognized by DIPP) are exempted from submission of EMD only. Relevant certificates should be submitted by the bidder in this regard to avail of exemption. Bid Security Declaration should be submitted by eligible MSEs/Startups on Company's letter head with company seal and signature of the authorized person as per Annexure-4.
5. The EMD may be forfeited/ Bank Guarantee/Insurance Surety Bond may be invoked:

- a) If the bidder withdraws/amends the bid during the period of bid validity (180 days from the date of opening of bid).
- b) If the bidder makes any statement or encloses any form which turns out to be false, incorrect and / or misleading at any time prior to signing of contract and/or conceals or suppresses material information; and / or
- c) The selected bidder withdraws his tender before furnishing the unconditional and irrevocable Performance Bank Guarantee.
- d) The bidder violates any of the provisions of the terms and conditions of this tender specification.
- e) In case of the successful bidder, if the bidder fails:
 - i To sign the contract in the form and manner to the satisfaction of Punjab & Sind Bank.
 - ii To furnish the Performance Bank Guarantee in the form and manner to the satisfaction of Punjab & Sind Bank.
 - iii Bank may proceed against the selected bidder in the event of any evasion, avoidance, refusal or delay on the part of the bidder to sign and execute the Purchase Order / Service Level Agreements or any other documents, as may be required by the Bank, if the bid is accepted.
 - iv The Execution of Bid Security Declaration/ Invocation of EMD may suspend participation of the Bidder in any tender in this Bank for three (03) years.
6. Bid securities of the unsuccessful bidders will be returned to them at the earliest after expiry of the final bid validity and latest on or before the 30th day after the award of the contract. The EMD of the selected bidder will be returned within 15 days after submission of Performance Security (PBG) and execution of Contract with the Bank.

6.11 Performance Bank Guarantee/Security Deposit (PBG)

1. The successful bidder/s should submit a Security Deposit / Performance Guarantee as specified in **Key Information within 30 days from the date of acceptance of Purchase Order.**
2. Security Deposit / Performance Guarantee should be submitted by way of Bank Guarantee in favor of Punjab & Sind Bank payable at Delhi / Bank Guarantee may be obtained from any of the Scheduled Commercial Banks (except Cooperative Bank, RRB & Punjab & Sind Bank) for an amount as mentioned in Section 1: KEY INFORMATION.
3. The selected bidder shall be responsible for providing the PBG for the duration of the contract (Including the extension) + claim period (12 months) of the Bank guarantees
4. The Bank Guarantee issued by the issuing Bank on behalf of Bidder in favor of Punjab & Sind Bank shall be in paper form as well as issued under the "Structured Financial Messaging System" (SFMS) sent to Punjab & Sind Bank, Sector 44 Branch, Gurgaon, IFSC PSIB0021509. Any bank guarantee submitted in physical mode, including EMD/bid guarantee which cannot be verifiable through SFMS will be summarily rejected.
5. The PBG applicable must be duly accompanied by a forwarding letter issued by the issuing bank on the printed letterhead of the issuing bank.
6. Security Deposit/Performance Bank Guarantee should be valid for the complete duration of contract period.

7. The selected bidder shall be responsible for extending the validity date and claim period of the Bank guarantees as and when it is due, on account of incompleteness of the project and contract period.
8. If the Contract is extended, the selected bidder has to submit fresh PBG (in addition to existing PBG) for 5% of the extended Contract value and period along with claim period and also execute fresh/extension of Contract with the Bank within 15 days from the date of issuance of Purchase Order for renewal.
9. In the event of the bidder committing a breach of the terms and conditions of the contract, Bank shall provide a cure period of 30 days and thereafter invoke the PBG, if the bidder is unable to service the contract for whatever reason.

6.12 No commitment to accept lowest or any bid

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

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

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

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

6.14 Correction of Errors

Bidders are advised to exercise greatest care in entering the pricing figures. No corrigendum or requests for prices to be corrected will be entertained after the bids are opened. If there are any corrections in the bid document, the authorized signatory should initial them all, failing which the figures for such item shall not be considered. Discrepancies in bids will be corrected as follows:

1. Where there is a discrepancy between the amounts in figures and in words, the amount in words shall prevail.

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

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

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

6.15 Soft copy of tender document

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

The bidder is advised to check the contents of the downloaded copy for correctness against the printed copy of the tender document. The printed copy of the tender document shall be treated as correct and final, in case of any errors in the soft copy.

6.16 Bid validity period

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

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

6.17 Pre-bid meeting

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

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

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

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

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

Participation in the Pre-Bid Meeting shall be restricted to duly authorized representatives of the bidder. The bidder shall submit an authorization letter, duly signed by its authorized signatory, for each representative attending the meeting. Additionally, the bidder shall share the names, designations, organization details, mobile numbers, and email addresses of the attendees with the Bank at least one (1) working day prior to the date of the Pre-Bid Meeting. The Bank reserves the right to deny participation to representatives whose details have not been communicated within the stipulated timeline.

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

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

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

6.18 Amendment to RFP Contents

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

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

6.19 Disqualification

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

6.20 Fixed Price

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

6.21 Project Execution

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

6.22 Confidentiality of the Bid Document

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

7 SCOPE OF WORK

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

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

The objective is to:

- Achieve end-to-end visibility and control over security events,
- Minimize attack surface through proactive threat detection and prevention,
- Ensure compliance with regulatory frameworks such as RBI Cybersecurity Framework, Government of India Guidelines, DPDP Act, ISO 27001, and other applicable mandates,
- Support the Bank's digital & Cyber transformation initiatives without compromising on security or performance.

The Bank's approach is aligned with global standards and best practices such as CERT-In Guidelines, **NIST Cybersecurity Framework, MITRE ATT&CK, and Zero Trust Architecture (ZTA)**. Solutions proposed under this RFP must integrate seamlessly into the Bank's existing ecosystem, ensure high availability and scalability, and provide centralized management, analytics, and automated response capabilities.

As part of this RFP, the Bank is seeking to procure the following solutions to strengthen its IT security infrastructure and enhance overall cyber posture:

1. Anti-Distributed Denial of Services (Anti-DDoS)
2. SSL Orchestrator along with packet broker
3. DNS protection (Internal DNS Security)
4. Web Gateway
5. Zero-Day Attack Protection at Endpoint and network/Anti-APT
6. Zero Trust Network Access (ZTNA)
7. Data Loss Prevention (DLP)
8. Information/Digital Right Management
9. Database Activity Monitoring
10. Mobile SDK

11. Host IPS including Application Change Control (HIPS)
12. Web Application Firewall (WAF)
13. Centralized key management solution
14. Certificate Lifecycle management
15. Identity & Access Management Solution
16. Multi Factor Authentication
17. Privilege Identity/Access Management
18. DNS Security Services (Internet-Facing DNS Security Services)
19. Cloud Access Security broker (CASB)
20. AI Security
21. SBOM, CBOM, AIBOM & QBOM

7.1 IT Security Solution & Services

To safeguard the bank's digital infrastructure and ensure robust cyber posture, the proposed cybersecurity solutions must comprehensively address all seven critical security layers (Perimeter, network, endpoint, application, data, identity, and compliance).

The bidder will be responsible for delivering and implementing these solutions at the locations as defined to safeguard and protect the data, IT assets of the bank deployed at DC, DR and other locations of the bank: -

A. Perimeter & Network Security

Solution Name	Use Case	Deployment location
Anti DDoS Solution	To protect digital banking services from volumetric denial-of-service (DoS/DDoS) attacks by detecting and mitigating abnormal traffic surges at the perimeter.	On-Premises at DC & DR
SSL Orchestrator with Network Packet Broker	To decrypt, inspect, and re-encrypt SSL/TLS traffic for deep packet inspection, ensuring visibility into encrypted threats across the network.	On-Premises at DC & DR
DNS Protection	To secure DNS infrastructure against spoofing, tunnelling, hijacking, and other DNS-based attacks by validating DNS queries and responses.	On-Premises at DC & DR
Web Gateway Solution	To ensure safe and compliant internet access across its network and remote endpoints. This solution should enable web traffic filtering, content control, user authentication, malware	On-Premises at DC & DR

Solution Name	Use Case	Deployment location
	protection, and threat prevention, with policy-based governance and consolidated reporting	
Zero-Day Attack Protection (Endpoint & Network)	To safeguard against sophisticated threats such as zero-day, stealth, and infiltration attacks across both network and endpoint levels	On-Premises at DC & DR
Zero Trust Network Access	To implement continuous risk-based access validation for remote users, enforcing zero trust principles with device posture checks and granular access control.	- Data Plane of the solution should be dedicatedly On-premises - OEM deploys other components per architecture.

B. Endpoint Security

Solution Name	Use Case	Deployment Model
Cloud Access Security Broker (CASB)	To provide centralized visibility, governance, and security for SaaS, PaaS, and IaaS applications by enforcing data protection, access control, Shadow IT discovery, user behaviour monitoring, threat detection, and regulatory compliance across cloud environments.	On-Cloud/Hybrid/On-premises at DC & DR
DLP (Data Loss Prevention)	To prevent unauthorized transfer, leakage, or exposure of sensitive customer or financial data through email, endpoints, USB, or other exfiltration channels.	On-Premises at DC & DR
DRM (Digital Rights Management)	To enforce policy-based access controls, usage restrictions, and encryption on sensitive files and documents, ensuring protection during storage and sharing.	On-Premises at DC & DR

C. Data Security

Solution Name	Use Case	Deployment Model
---------------	----------	------------------

DAM (Database Activity Monitoring)	To provide real-time monitoring, auditing, and alerting of all privileged and non-privileged activities across critical databases, supporting compliance and threat detection.	On-Premises at DC & DR
Mobile SDK (Software Development Kit)	To integrate mobile application security controls (e.g., jailbreak detection, code obfuscation, secure storage) within the bank's apps during development lifecycle.	On-Premises at DC & DR

D. Application Security

Solution Name	Use Case	Deployment Model
HIPS (Host-based Intrusion Prevention System)	To detect and block malicious activity at endpoint level through behavioural analysis, signature matching, and anomaly detection on host systems.	On-Premises at DC & DR
Web Application Firewall (WAF)	To protect publicly exposed banking web applications from OWASP Top 10 attacks, bots, and layer 7 threats using rule-based and AI-driven detection.	On-Premises at DC & DR
Centralised Key Management	To ensure centralized lifecycle management of cryptographic keys, supporting secure generation, rotation, archival, and revocation across enterprise systems.	On-Premises at DC & DR
Certificate Lifecycle Management	To centrally discover, issue, renew, revoke, monitor, and manage digital certificates across the Bank's IT infrastructure, applications, cloud, and network devices.	On-Premises at DC & DR
S-BOM, CBOM, AIBOM and QBOM	To provide centralized discovery, inventory,	On-Premises/ On-Cloud/Hybrid at DC & DR

Solution Name	Use Case	Deployment Model
	governance, and continuous monitoring of software components, cryptographic assets, AI models, and quantum-vulnerable dependencies across the Bank's IT environment. The solution shall identify security, compliance, software supply chain, cryptographic, AI, and post-quantum risks while supporting vulnerability management, crypto-agility, AI governance, and regulatory compliance through a unified Bill of Materials (BOM) framework.	

E. Management Layer and Security

Solution Name	Use Case	Deployment Model
IDAM (Identity and Access Management)	To manage user identities, enforce role-based access controls (RBAC), enable least privilege, and ensure secure provisioning and de-provisioning across IT assets.	On-Premises at DC & DR
Multi-Factor Authentication	To strengthen authentication processes by implementing layered identity verification (e.g., OTP, biometric, hardware token) beyond traditional passwords.	On-Premises at DC & DR
PIM (Privileged Identity Management)	To control, monitor, and audit activities of users with elevated privileges through session recording, approval workflows, and time-bound access.	On-Premises at DC & DR
AI Security	To securely govern, monitor, and control enterprise AI/Generative AI usage by providing AI gateway, prompt inspection, data leakage prevention, AI firewall, model access control, guardrails, prompt injection	On-Premises at DC & DR

Solution Name	Use Case	Deployment Model
	protection, model risk management, and centralized policy enforcement for all AI services and enterprise LLMs.	

- The successful bidder shall provide end-to-end services for the proposed IT and Cyber Security solutions, including design, supply, implementation, integration, migration, training, documentation, monitoring, OEM coordination, warranty, and post-warranty support during the contract period.
- The bidder shall be fully responsible for the successful deployment, operation, maintenance, security, performance, and support of the proposed solution and all associated components, without any additional cost to the Bank.

Note:

1. The implementation of each solution, including design, installation, configuration, integration, migration, testing, and Go-Live, shall be performed by OEM. The bidder shall arrange OEM resources, coordinate implementation activities, and ensure timely project completion.
2. Upon successful implementation, the respective OEM shall provide a certificate confirming that the solution has been deployed by OEM and meets the requirements specified in the RFP and SRS.
3. Roles and Responsibilities (Indicative):
 - a. System Integrator (Bidder): Supply the proposed solutions, provide onsite L1/L2/L3 support resources, manage the project, and coordinate with OEMs.
 - b. Solution OEM: Deploy, configure, integrate, test, commission, and migrate data/logs from existing solutions, and ensure successful implementation of the proposed solution.
4. Security tools, agents, collectors, and connectors shall also be deployed in the Bank's cloud/VPC environment, wherever applicable, to ensure consistent visibility, monitoring, logging, and protection across cloud and on-premises infrastructure.
5. The bidder shall be responsible for implementation, integration, migration, upgrades, patching, troubleshooting, health checks, backups, audit support, documentation, SOP creation, and lifecycle management of all proposed IT Security solutions during the contract period.
6. In case of implementation delays, the bidder shall ensure seamless takeover and transition of in-scope existing security solutions and services from the incumbent vendor without disruption to Bank operations at no additional cost to the bank.
7. All proposed solutions shall support real-time integration, event correlation, orchestration, and automated response capabilities to enable unified security operations and effective threat management.
8. The proposed solutions shall provide dynamic, customizable dashboards and reports with analytical and actionable insights for effective monitoring, governance, and decision-making

9. The proposed solution, tools and IT Infrastructure must be OEM-supported, production-grade and stable (GA release).
10. All supporting and underlying software components, including but not limited to databases, application servers, web servers, middleware, and other dependencies required for the proposed solution, shall be enterprise licensed version & OEM-supported, community version shall not be proposed, and shall form part of the bidder's overall solution offering for both on-premises and cloud deployments.

Cyber Security Incident / Data Breach

- a. The Bidder shall immediately, and in any event not later than six (6) hours from becoming aware of any actual, suspected or reasonably suspected cyber security incident, data breach, unauthorised access, malware/ransomware incident, compromise of credentials, leakage/loss of Bank Data or security vulnerability affecting the Bank, notify the Bank through the designated incident reporting mechanism.
- b. The Bidder shall immediately take all necessary steps for containment, mitigation, investigation, eradication and recovery of the incident and shall ensure that the incident does not result in further compromise of the Bank's systems or data.
- c. The Bidder shall preserve all logs, records, forensic evidence, system images and other relevant information and shall not destroy, alter or overwrite such evidence.
- d. The Bidder shall provide full cooperation to the Bank, its auditors, investigators, RBI, CERT-In and other competent regulatory/statutory authorities.
- e. The Bidder shall provide a preliminary incident report immediately and a detailed Root Cause Analysis and corrective action report within the timeline prescribed by the Bank.
- f. All reasonable costs incurred by the Bank for investigation, containment, remediation, restoration, forensic audit, data recovery and other measures necessitated by an incident attributable to the Bidder/OEM/subcontractor shall be recoverable from the Bidder

7.2 RACI (Responsible, Accountable, Consulted, Informed)

#.	Activity	Bidder	OEM	Bank
1	Requirement Analysis	A,R	R	R,A,C,I
2	Solution & System Design	A,R	R	C,I
3	Installation, Integration & Implementation	A,R	R	C,I
4	Configuration, Policy & Rule Management	A,R	R	C,I
5	Documentation & Knowledge Transfer	A,R	R	C,I
6	Testing, UAT & Go-Live Support	A,R	R	R,C,I
7	Deployment & Go-Live	A,R	R	C,I
8	Facility Management & Resource Management	A,R	C	I

#.	Activity	Bidder	OEM	Bank
9	IT Security Operations	A,R	C	I
10	Business Continuity & DR Support	A,R	C	I
11	Architecture Review & Assessment	A,R	R	R,C,I
12	Closure of Audit, Assessment & Review Observations	A,R	R	R,C,I
13	Change, Release & Impact Management	A,R	R	C,I
14	Incident, Problem & Service Management	A,R	R	A,C,I
15	OEM Coordination & Escalation Management	A,R	R	I
16	Product Upgrades, Patches & Hotfixes	A,R	R	I
17	Security Health Checks & Optimization	A,R	R	R,C,I
18	Regulatory, Audit & Compliance Support	A,R	C	R,C,I

Legend:

R – Responsible | **A** – Accountable | **C** – Consulted | **I** – Informed

7.3 Functional Requirements

7.3.1 Perimeter & Network Security

7.3.1.1 Anti-Distributed Denial of Service (Anti-DDoS)

Bidder should propose an Anti-DDoS solution to effectively protect its internet-facing services from advanced Distributed Denial of Service (DDoS) attacks targeting both network and application layers.

The solution must offer end-to-end protection against a wide range of threats, including but not limited to UDP Floods, ICMP Floods, SYN Floods, Smurf attacks, HTTP Floods, Zero-day exploits, and TCP exhaustion. It should ensure seamless access for legitimate users while delivering real-time threat detection, automated mitigation, and robust performance.

The system must also integrate smoothly with the Bank's existing security infrastructure and provide detailed reporting to support security operations and regulatory compliance. Additionally, it should safeguard against SSL/TLS-based attack vectors, including those targeting dedicated SSL/TLS offload devices, ensuring continued availability and reliability of critical banking applications.

Architecture, Modules & Deployment:

- Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: Anti-DDoS NGFW.

Key Deliverables:

- DDoS protection reports including:
 - Attack detection and mitigation reports
 - Traffic analysis and anomaly detection reports
 - Bandwidth utilization and attack volume statistics
 - Geographic attack source analysis
 - SSL/TLS vulnerability protection status
- SOPs and documents
- Custom Dashboards

4. Fine-tuned models
5. Baseline for users and entities

7.3.1.2 SSL Orchestrator Tool (along with Packet Capture)

The Bank intends to implement an SSL Orchestrator and Packet Capture (PCAP) solution to strengthen its cybersecurity posture by enabling deep inspection of encrypted traffic. This includes decrypting, analyzing, and monitoring SSL/TLS communications in real-time to detect malware, phishing attempts, data exfiltration, and policy violations. The solution must preserve data privacy, align with regulatory compliance, and support audit readiness through full traffic visibility and replay capabilities.

The solution should enable complete packet capture, recording all network traffic including headers and payloads without any data loss, and support replay functionality to facilitate risk analysis through integration with other security tools. Traffic capture must be supported via port mirroring, and the bidder shall propose optimal placement strategies to ensure maximum visibility and effectiveness.

Architecture, Modules & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: SSL Orchestrator.

Key Deliverables:

1. Fully configured SSL Orchestrator and PCAP solution with centralized management console and high availability setup.
2. Service chaining configuration with defined traffic flows and integrated inline tools (IPS, WAF, NGFW, etc.).
3. Complete documentation including policy matrix, traffic steering guides, exception handling rules, and SSL certificate tracking procedures.
4. Operational and training manuals covering decrypted traffic monitoring, certificate management, incident handling, and packet replay.
5. Reports including:
 - a. SSL traffic volume statistics
 - b. Packet capture and replay audit logs
 - c. Policy violation reports
 - d. Certificate expiry alerts
 - e. Tool-chain inspection results
6. DR validation report and integration checklist with existing security infrastructure.
7. Privacy and compliance validation ensures decrypted data handling adheres to applicable guidelines.
8. Escalation matrix and SOPs for issue handling, policy updates, and change requests.

7.3.1.3 DNS protection (Internal DNS Security)

The Solution should enable bank in securing DNS communications across its enterprise infrastructure, enhancing visibility into DNS activities, reducing the risk of DNS-based attacks, and enabling early

detection and response to cyber threats. The solution shall support the Bank in protecting critical information assets, ensuring secure access to digital services, improving cyber resilience, and meeting regulatory, audit, and security governance requirements across on-premises and cloud environments.

The proposed solution should identify and block access to malicious, suspicious, phishing, and unauthorized domains, thereby reducing the risk of credential theft, malware infections, and other cyber threats. The solution shall monitor and analyze DNS traffic, detect and prevent DNS tunneling, command-and-control (C2) communications, and malicious DNS requests that may be indicative of malware activity or data exfiltration attempts.

The solution should provide DNS activity logging, behavioral analytics, threat intelligence integration, anomaly detection, and real-time alerting to support proactive threat detection, incident investigation, and integration with the Bank's SOC and SIEM platforms.

Architecture, Modules & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: DNS Protection.

Key Deliverables:

1. Installation and configuration report including:
 - a. Network integration validation
 - b. Connectivity with SIEM, SOAR, Zero Day attack, TIP/Feed, Firewall, and DLP
2. Operational SOPs for:
 - a. Incident response at the DNS layer
 - b. Threat detection and mitigation steps
 - c. Update and patching protocols
3. Monitoring and vulnerability scan reports
4. Administrative documentation and user access matrix
5. Escalation and support contact matrix

7.3.1.4 Web Gateway Solution

The Bank intends to deploy a comprehensive Web Gateway Solution (Secure Web Gateway) solution to ensure safe and compliant internet access across its network and remote endpoints. This solution should enable web traffic filtering, content control, user authentication, malware protection, and threat prevention, with policy-based governance and consolidated reporting.

The solution must support a hybrid deployment model (cloud and on premises), provide advanced web proxy capabilities, and integrate with the Bank's DLP, SIEM, and IT Security & IT systems to enhance overall web security posture and threat intelligence.

The Solution should provide content filtering, web control, identify malicious payloads and to restrict access for Bank users accessing internet. Secure Web Gateway should have the capability to authenticate

users, filter web traffic, identify cloud application usage and deliver threat prevention. Further, the solution should provide consolidated policy management and reporting.

Architecture, Modules & Deployment

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: Web Gateway.

Bidder/OEM Responsibility:

1. The OEM shall install, configure, and integrate the Web Gateway solution in the Bank's environment (on-premises and cloud).
2. The OEM is responsible for seamless integration with security infrastructure including DLP, SIEM, and IT Security solutions.
3. OEM to ensure policy setup, system tuning, and security configuration are aligned with the Bank's cybersecurity framework.
4. OEM to create, configure and define reverse proxy scenarios, terminal services integration, and custom filtering rules set up.
5. Integrate the solution with required IT Security solutions

Key Deliverables:

1. Technical documentation includes:
 - a. Web filtering rule sets
 - b. Proxy setup guides
 - c. Integration documents for DLP, SIEM, and IT Security solutions
2. Deployment deliverables such as:
 - a. Reports
 - b. Configuration validation logs
 - c. Hybrid connectivity test results
3. Policy and classification framework including:
 - a. URL category mappings
 - b. Application control and reputation block lists
 - c. Website classification accuracy metrics
4. Support documentation:
 - a. Escalation matrix
 - b. SOPs for administration and reporting
 - c. Threat prevention configuration and use cases

7.3.1.5 Zero-Day Attack Protection at Endpoint and network

To strengthen its cyber defense mechanisms, the Bank plans to implement a Zero Day Attack Protection at Endpoint and network solution. The objective is to safeguard against sophisticated threats such as zero-day, stealth, and infiltration attacks across both network and endpoint levels. The solution should offer real-time protection, deep analysis, and automated response capabilities. Integration with the Bank's existing security infrastructure is essential.

Architecture, Modules & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: Zero Day Attack Protection.

Bidder/OEM Responsibility:

1. Install and configure the solution as per the Bank's requirements.
2. Identify and recommend necessary changes in network architecture or infrastructure to accommodate the solution
3. Ensure integration with Bank's IT & Cyber Security systems but not limited to
 - a. SIEM
 - b. SOAR
 - c. UEBA
 - d. XDR
 - e. SOC-BIG Data Lake
 - f. Firewall
 - g. TIF
 - h. Any other as required by bank
4. Maintain compatibility with all major operating systems
5. Coordinate with the Bank's security teams during investigations and forensic assessments

Key Deliverables:

1. Fully deployed Zero-Day Attack Protection at Endpoint and network solution covering both network and endpoint layers
2. Integration report with the platforms
3. Documentation of recommended infrastructure changes for effective deployment
4. 24x7 monitoring and malware scanning for critical websites
5. Incident response plan including rapid action and forensics procedures
6. Training and handover to the Bank's security/IT team on solution operation and event handling

7.3.1.6 Zero Trust Network Access

The Bank intends to implement a comprehensive Zero Trust Network Access (ZTNA) solution to enhance secure, efficient, and seamless access for remote users across its growing and complex network environment.

The solution must provide secure, fast, and reliable access to internal applications, irrespective of user location, while enforcing strong authentication and continuous device posture checks including configuration compliance, patch status, antivirus updates, and OS activation.

The primary objective is to significantly reduce the attack surface, prevent unauthorized access, and safeguard critical digital assets such as servers, endpoints, and sensitive data.

Architecture, Modules & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: ZTNA.

Bidder/OEM Responsibility:

1. OEM to Supply, deploy, and configure the Zero Trust solution in line with Bank's requirements
2. OEM to Integrate the solution for central visibility and automated response but not limited to:
 - a. IDAM
 - b. XDR
 - c. Firewall
 - d. SIEM
 - e. SOAR
 - f. SOC-Big Data Lake
 - g. DLP
 - h. CSPM
 - i. TIP
 - j. UEBA
 - k. PIM/PAM
 - l. Any other as specified by bank
3. Ensure support for application and device posture validation, with timely updates and tuning
4. OEM to define segmentation rules, user access policies, and security parameters aligned with best practices
5. OEM to integrate with the Bank's infrastructure including Patch Management, Network Access Control (NAC), ITSM, and Identity Management Systems to support centralized visibility, policy enforcement, and automated response.

Key Deliverables:

1. Successfully deployed Zero Trust access solution, with all required integrations
2. Configuration documents, including segmentation rules and posture-checking parameters
3. Policy management dashboard setup and documentation for centralized control
4. Training and support for IT/security administrators on solution features and operations
5. Integration reports confirming connectivity with SIEM and SOAR solutions
6. Discovery report of internal applications identified by AI/ML engine for policy mapping

Notwithstanding anything contained anywhere in this RFP, the Selected Bidder shall be the principal contracting party and shall remain fully, jointly and severally responsible and liable to the Bank for performance of the entire Scope of Work, including all activities performed by the OEM(s), subcontractors, agents, employees or other third parties. The Bank shall not be required to pursue or enforce any remedy separately against any OEM or subcontractor.

7.3.2 End Point Security

7.3.2.1 Cloud Access Security broker (CASB)

The Bank requires a comprehensive Cloud Access Security Broker (CASB) solution to provide centralized visibility, governance, and security for the Bank's usage of SaaS, PaaS, and IaaS cloud services.

It shall seamlessly integrate with the Bank's Identity Provider (IdP), SIEM, SOAR, DLP, XDR, Threat Intelligence Platform (TIP), and IT & SOC Security ecosystem while ensuring that the data plane remains dedicatedly deployed On-Premises at the Bank's DC & DR, with centralized management, reporting, and policy administration.

1. Architecture, Modules & Deployment: Proposed solution should comply with the requirement mentioned in Appendix 1: Functional Compliance Sheet, Sheet Name: CASB.

Key Deliverables:

1. End-to-end deployed and operational CASB solution providing visibility and security across all sanctioned and unsanctioned cloud applications, SaaS, PaaS, and IaaS environments.
2. Centralized CASB management console with real-time dashboards, policy management, alerting, reporting, and audit capabilities.
3. Integration with Identity Provider (AD/LDAP/Azure AD), SIEM, SOAR, DLP, XDR, Threat Intelligence Platform (TIP), Secure Web Gateway (SWG), and IT Security & SOC platforms.
4. Comprehensive cloud security posture, user activity, policy violation, data exposure, Shadow IT, and compliance reports with customizable dashboards.
5. SOPs, administration guides, architecture documents, policy configuration documents, and knowledge transfer/training sessions for Bank personnel on CASB operations, monitoring, policy management, and incident response.

7.3.2.2 Data Loss Prevention

The Bank requires a comprehensive Data Loss Prevention solution to secure its sensitive information across endpoints, network channels, and storage systems throughout all locations. The solution must provide advanced capabilities to detect, monitor, and prevent unauthorized disclosure of confidential data such as customer information, financial records, and intellectual property.

It should deliver real-time protection across multiple channels including email, web, removable media, and file transfers, while providing centralized management, detailed incident reporting, and seamless integration with the Bank's IT & SOC security infrastructure to ensure compliance with regulatory requirements and protection against data breaches.

1. Architecture, Modules & Deployment: Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: DLP.

Key Deliverables:

1. End-to-end deployed and operational DLP solution, covering all required channels (endpoint, email, network, USB, web, SaaS) and locations (DC, DR, branches, remote users).
2. DLP agent deployment and coverage report, listing devices, installation status, policy versions, last sync, and enforcement status.
3. Centralized DLP dashboard with real-time monitoring and reporting capabilities.

4. Integration with email systems for policy enforcement and quarantine handling.
5. SOPs, documentation, and training sessions for Bank personnel on DLP operations and incident response.
6. Reports on policy effectiveness, including blocked events, false positive ratios, rule tuning recommendations, and coverage metrics
7. Detailed data classification matrix and policy mapping document covering data types, risk level, channels, and enforcement actions

7.3.2 Information/Digital Right Management

The Bank intends to implement an Information/Digital Rights Management (IRM/DRM) solution to secure the sharing of sensitive and confidential information both within and outside the organization. The Bank is exposed to risks of data misuse and unauthorized access in the normal course of business. The solution must ensure encryption, user-level access control, classification enforcement, and usage restrictions irrespective of how or where the data is accessed via email, cloud platforms, collaboration tools, removable media, or external networks. The solution should enable the end user to define user rights for the protection of files / folders and emails. This will facilitate enhanced control of access and usage rights for the same, both within and outside the organization.

Modules, Architecture & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: DRM.

Key Deliverables:

1. Configuration documents including:
 - i. Data classification rules
 - ii. Access permission matrices
 - iii. SIEM integration configurations
2. Training materials and operational guides covering:
 - i. User rights management
 - ii. Document/email protection workflow
 - iii. Admin enforcement of policies
 - iv. Troubleshooting procedures
3. Support documentation for:
 - i. Patch and upgrade schedules
 - ii. Escalation matrix for L1, L2, L3 support
 - iii. Incident response and resolution logs
4. Reports such as:
 - i. Rights management activity logs
 - ii. Policy enforcement summaries
 - iii. Integration audit with SIEM
5. Comprehensive operational and audit trail reports for all modules
6. Automated and scheduled report generation with configurable templates

7. Email alerts/notifications at key transaction stages
8. Online access to real-time reports via secure dashboard
9. Full event and access logging with change tracking
10. Pre-built query options for non-technical users
11. Support for regulatory/compliance reporting as per Bank-defined frequency and format

7.3.3 Data Security

7.3.3.1 Database Activity Monitoring

To enhance its data protection framework, the Bank proposes to implement a robust Database Activity Monitoring (DAM) solution. The solution is expected to provide continuous visibility into all database interactions, including local access, application queries, and remote connections, to detect and respond to unauthorized or unusual activity in real time. This will significantly reduce the risk of data breaches, insider threats, and policy violations.

In addition, the DAM solution should support scheduled vulnerability assessments, help identify misconfigurations or weak access controls, and facilitate prompt remediation through patching or virtual patching. Given the Bank's use of diverse database platforms and versions, the solution must ensure compatibility and seamless deployment across its server environment. This initiative will act as a proactive control to safeguard sensitive financial and customer data, maintain compliance with regulatory requirements, and strengthen the overall cybersecurity posture of the Bank.

Modules, Architecture & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: DAM.

Key Deliverables:

1. Regular reports including:
 - i. Database activity monitoring reports
 - ii. Policy violation and access control deviation reports
 - iii. Sensitive data discovery reports
 - iv. Vulnerability assessment and patch management reports
 - v. Compliance status reports for various standards (Cert-In, RBI, PCI-DSS etc.)
2. SOPs and documents
3. Custom Dashboards
4. Fine-tuned models
5. Baseline for users and entities

7.3.3.2 Mobile SDK

The Bank intends to implement a Mobile Software Development Kit (SDK) to securely integrate advanced threat detection, behavioural analytics, and application protection within its applications. The

SDK will enable key features such as biometric authentication, device binding, secure PIN input, fraud detection, transaction risk scoring, and in-app messaging. It will ensure that all security events originating from the mobile application are captured and correlated with the Bank's central security infrastructure for improved monitoring and response.

In addition to strengthening security, the SDK will support faster deployment of digital services, deliver a consistent user experience across platforms, and ensure compliance with regulatory requirements such as RBI's cybersecurity guidelines. This flexible and customizable framework will allow the Bank to maintain control over critical functionalities while enhancing the overall usability, performance, and trustworthiness of its mobile banking channel.

Modules, Architecture & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: Mobile SDK.

Key Deliverables:

1. Delivery of the Mobile SDK library along with integration guides and developer documentation.
2. Successful integration of the SDK into the Bank's mobile application, including validation of threat detection and security event generation.
3. End-to-end integration with the Bank's SIEM and SOAR platforms for centralized alerting and correlation.
4. Periodic updates and patches for the SDK to address evolving mobile threats and maintain compatibility with updated mobile OS versions.
5. MIS reports and dashboards capturing the telemetry and threat insights generated by the SDK.

7.3.4 Application Security

7.3.4.1 Host IPS including Application Change Control

The Bank intends to implement a Host-based Intrusion Prevention System (HIPS) to strengthen its endpoint and server-level security. The proposed solution shall provide real-time monitoring, detection, and prevention of malicious activity at the host level, including unauthorized changes to system files, registry entries, application configurations, and memory processes.

The HIPS solution is required to enhance the Bank's protection against advanced threats such as zero-day attacks, fileless malware, and privilege escalation attempts that may bypass traditional network perimeter defences. It is expected to provide behavioural analysis, signature-based detection, and policy enforcement capabilities across all critical infrastructure components including core banking servers, database servers, internet-facing applications, and privileged user endpoints.

Architecture, Modules & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: HIPS.

Key Deliverables:

1. The service delivery (SLA Management) and periodic reporting through automated dashboards.
2. Host baseline profiling, including identification of approved applications, services, binaries, and configurations for various endpoint/server types and defining enforcement policies accordingly.
3. Deployment and configuration of HIPS agents on all in-scope systems, along with periodic validation of agent status, policy adherence, and system compatibility.
4. Creation and continuous fine-tuning of HIPS rules and policies tailored to the Bank's environment, including:
 - a. Host behaviour monitoring rules
 - b. Application control and integrity policies
 - c. Block/allow lists for executables and scripts
 - d. Detection of anomalous and unauthorized changes
5. Integrated dashboard with customized views depending on role of the user and provide an online secured portal (web-based dashboard) for viewing real-time incidents/events, alerts, status of actions taken, etc. The views required by Bank are as follows:
 - a. Top Management (Organization level view)
 - b. Department Heads (View the data associated with their function group/business line)
 - c. CISO
 - d. System Administrator (View of systems associated with this administrator)
 - e. Network / Security Administrator (View of devices/equipment for which they are an administrator)
 - f. Application Administrator (View of systems associated with this administrator)
 - g. Auditor (Internal Auditors, IT Auditors, ISO Certification Auditor, or any other authorized official of the organization).
6. Report highlighting the following:
 - a. Number of endpoints with active HIPS agents
 - b. Number of blocked attacks or unauthorized actions
 - c. Application change violations (authorized vs unauthorized changes)
 - d. False positives vs true positives in host-based detections
 - e. Policy compliance status across the infrastructure
 - f. Devices with no recent activity or unresponsive agents
 - g. Summary of quarantined processes or blocked executables

7.3.4.2 Web Application Firewall

The Bank requires a comprehensive Web Application Firewall solution to protect its web applications and APIs from sophisticated cyber-attacks and vulnerabilities.

The solution must provide advanced protection against OWASP Top 10 vulnerabilities, API threats, and emerging attack vectors, while ensuring minimal performance impact on application delivery.

It should deliver real-time detection and mitigation capabilities, centralized management, integration with existing security infrastructure, and detailed reporting for security operations and compliance purposes, all while maintaining high availability to support the Bank's critical customer-facing applications.

Architecture, Modules & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: WAF.

Key Deliverables:

1. Implementation and configuration of WAF covering OWASP Top 10, API, and CVE-based threat protection.
2. Integration with third-party vulnerability scanners.
3. Centralized management console with reporting and alerting capabilities.
4. Integration with SIEM and SOAR solutions.
5. Deployment of advanced bot detection and API protection mechanisms.

7.3.4.3 Centralized key Management solution

The Bank intends to implement a Centralized Key Management Solution (KMS) to ensure secure, efficient, and policy-driven management of cryptographic keys across its IT environment. A Centralized Key Management Solution helps the Bank securely store, generate, rotate, and manage encryption keys used across different security tools (like SSL Orchestrator, DLP, WAF, etc.). The solution shall enable lifecycle management of encryption keys including generation, distribution, rotation, archival, and revocation for both on-premise and cloud-based systems without altering the configuration of target systems or infrastructure.

The solution must enhance data confidentiality, ensure regulatory compliance (including PCI-DSS and ISO 27001), reduce operational risks, and provide visibility and control over key-related operations. It should support browser-based centralized administration, standards-based interoperability (e.g., KMIP), robust access control with segregation of duties, and full audit logging.

Modules, Architecture & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: KMS.

Key Deliverables:

1. Fully deployed and operational KMS with integration across environments

2. Documentation of procedures for key generation, distribution, rotation, expiry, revocation, archival, and destruction.
3. Real-time and historical logging of key usage and access, aligned with regulatory and internal audit requirements.
4. UAT, security clearance, and final project sign-off certificates
5. Compliance audit reports for PCI-DSS, ISO 27001
6. Role-based access policy documentation and enforcement reports
7. SOPs, operational manuals, and escalation/resolution matrix
8. Monitoring dashboard, audit trail logs, and certificate/key expiry alerts

7.3.4.4 Certificate Lifecycle Management

The Bank requires a comprehensive Certificate Lifecycle Management (CLM) solution to centrally discover, issue, renew, revoke, monitor, and manage digital certificates across its on-premises, cloud, hybrid, network, security, and application infrastructure. The solution shall provide complete visibility into certificate inventories, automate certificate lifecycle operations, eliminate certificate-related outages, enforce cryptographic policies, and ensure compliance with regulatory and security requirements.

Modules, Architecture & Deployment:

Proposed solution should comply with the requirement mentioned in **Appendix 1: Functional Compliance Sheet, Sheet Name: Certificate Lifecycle Management (CLM)**

Key Deliverables:

1. End-to-end deployed and operational Certificate Lifecycle Management solution
2. Comprehensive certificate discovery and inventory report, including certificate owners, issuing CAs, validity, key lengths, cryptographic algorithms, expiry status, risk classification, and compliance status.
3. Centralized CLM management console with certificate issuance, enrolment, renewal, revocation, expiry alerts, workflow approvals, policy enforcement, dashboards, and reporting.
4. Certificate lifecycle workflows with policy-based approvals, notifications, audit trails, certificate replacement, and outage prevention mechanisms.
5. SOPs, architecture documents, administration guides, operational runbooks, and training sessions for Bank personnel covering certificate lifecycle operations, governance, troubleshooting, incident response, and cryptographic policy management.

7.3.4.5 S-BOM, C-BOM, AI-BOM & QBOM

The Bank requires a comprehensive Software Bill of Materials (S-BOM), Cryptographic Bill of Materials (C-BOM), AI Bill of Materials (AI-BOM), and Quantum Bill of Materials (Q-BOM) solution to provide centralized discovery, inventory, governance, and continuous monitoring of software components, cryptographic assets, AI assets, and quantum-vulnerable dependencies across the Bank's IT environment. The solution shall identify software supply chain risks, known vulnerabilities, cryptographic weaknesses, AI model risks, licensing issues, and quantum-readiness gaps while supporting vulnerability management, crypto-agility, AI governance, regulatory compliance.

Architecture, Modules & Deployment:

Proposed solution should comply with the requirements mentioned in **Appendix 1: Functional Compliance Sheet, Sheet Name: S-BOM, C-BOM, AI-BOM & Q-BOM.**

Key Deliverables:

1. End-to-end deployed and operational S-BOM, C-BOM, AI-BOM, and Q-BOM solution covering enterprise applications, APIs, operating systems, containers, Kubernetes, cloud workloads, AI models, cryptographic assets, and software repositories.
2. Centralized management console providing real-time dashboards.
3. SOPs, architecture documents, operational runbooks, administration guides, policy documentation, and knowledge transfer/training sessions for Bank personnel covering BOM governance, software supply chain security, cryptographic governance, AI governance, and PQC migration planning

7.3.5 Management Layer Security

7.3.5.1 Identity & Access Management Solution

The Bank requires an Identity & Access Management (IDAM) solution to establish secure, centralized control over user identities, access rights, and authentication mechanisms across its IT ecosystem. The solution must provide capabilities for user lifecycle management, identity governance, access certification, and seamless integration with the Bank's Multi-Factor Authentication (MFA) solution.

It should support Single Sign-On (SSO), integration with multiple directories, and enforce role-based access controls while ensuring compliance with regulatory standards. The solution must be scalable, interoperable with core systems like HRMS, ITSM, and SIEM, and capable of operating in a high availability and disaster recovery setup.

Modules, Architecture & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: IDAM.

Key Deliverables:

1. Configuration documentation including:
 - i. Directory and domain integration details
 - ii. Identity lifecycle and access governance rules
 - iii. Integration setup with HRMS, ITSM, MFA, PAM, SIEM, SOAR and other tools & Infrastructures
2. Operational manuals and training documentation covering:
 - i. SSO setup and management
 - ii. User provisioning/de-provisioning
 - iii. Privileged account governance
 - iv. Alert and incident management
3. Reports covering:

- i. User and access certification status
- ii. Integration of health and connectivity logs
- iii. Identity governance and compliance reports

7.2.1.1. Multi Factor Authentication

The bank intends to implement a Multi-Factor Authentication (MFA) solution to enhance the security of its digital infrastructure by introducing an additional layer of authentication that goes beyond traditional username and password, ensuring that only authorized users can access critical banking systems, applications, and customer data. This is essential to protect against evolving cyber threats such as phishing, identity theft, and unauthorized access, while also ensuring compliance with regulatory requirements such as RBI guidelines, ISO 27001, and other industry standards aimed at safeguarding the integrity, confidentiality, and availability of financial systems.

The solution shall seamlessly integrate with the SIEM solution of the Bank. In case required, the Bidder shall provide all required support to integrate it with SIEM.

Modules, Architecture & Deployment:

1. Proposed solution should comply with the requirements mentioned in Appendix 1: Functional compliance sheet, Sheet Name: MFA.

Key Deliverables:

1. Fully deployed, configured, and integrated MFA solution across all identified systems, applications, and access points.
2. Integration of MFA with existing infrastructure including AD/LDAP, VPN, email, internet banking, core banking, remote access, cloud applications, and ITSM.
3. User provisioning and enrolment workflows, including support for various authentication factors (e.g., OTP, push notification, biometric, hardware token, mobile app).
4. Administrative dashboard with role-based access for monitoring, reporting, and policy enforcement.
5. High Availability and Disaster Recovery (DR) setup documentation, including validation results of failover authentication scenarios and restoration procedures.
6. Licensing and usage reports capturing number of deployed vs. available licenses, allocation status, and token/device inventory details.
7. Change management logs capturing version updates, configuration changes, rollback records, and software/firmware patch history relevant to the deployed MFA solution.

7.2.1.2. Privilege Identity Management (PIM)

The Bank intends to upgrade its existing Privileged Identity Management (PIM) solution to enhance control and security over privileged access across its critical IT infrastructure and enterprise applications. The upgraded solution must provide comprehensive privileged account management, including secure credential storage (password vaulting), real-time session monitoring, granular access control, and detailed audit trails to meet regulatory and internal compliance requirements. The

objective is to enforce least privilege access, enhance visibility, and ensure accountability of privileged activities across the Bank's IT ecosystem, helping to mitigate insider threats and prevent misuse of elevated privileges.

Modules, Architecture & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: PIM.

Key Deliverables:

1. OEM to provide SOPs, installation, configuration, and integration documents.
2. Support for creation of custom dashboards
3. Capability for fine-tuning behavior models
4. Baseline creation for privileged users and entities.
5. Out-of-the-box compliance reports (e.g., RBI, DPDP).
6. Custom report creation and scheduling.
7. Role-based access reporting capability.
8. Must generate reports including:
 - i. Privileged user activity
 - ii. Configuration changes
 - iii. Session/access logs
 - iv. Capacity utilization
 - v. Vault access history
 - vi. Integration and health status

7.3.5.2 DNS Security Services

The DNS Security services to secure internet-bound DNS traffic and protect users, systems, and applications from phishing, malware, ransomware, command-and-control (C2) communications, DNS tunneling, and other DNS-based threats. The solution shall provide real-time DNS monitoring, threat prevention, policy enforcement, visibility, reporting, and integration with the Bank's cyber & security ecosystem to strengthen the Bank's overall cybersecurity posture and cyber resilience.

The solution shall offer centralized visibility into DNS activities, policy-based controls, threat intelligence integration, logging, reporting, and seamless integration with the Bank's SOC ecosystem to enhance threat detection, incident response, cyber resilience, and regulatory compliance.

Architecture, Modules & Deployment:

1. Proposed solution should comply with the requirement mentioned in Appendix 1: Functional compliance sheet, Sheet Name: DNS Services.

Key Deliverables:

1. DNS policy enforcement report including blocked domains, alerts, and violations.

2. Integration logs with SIEM and other security tools.
3. SOPs for monitoring, threat response, and alert tuning.
4. Dashboard access for DNS analytics, incident tracking, and compliance reporting.
5. Periodic audit trail reports for regulatory and internal governance purposes.
6. Anomaly Detection- Alert on DNS spikes, beaconing patterns, or unclassified domain activity

7.3.5.3 AI Security

The Bank requires a comprehensive **AI Security & Guardrails** solution to securely govern, monitor, and protect the usage of Artificial Intelligence (AI), Generative AI (GenAI), Large Language Models (LLMs), AI agents, and AI-powered applications across the Bank.

Architecture, Modules & Deployment

Proposed solution should comply with the requirements mentioned in **Appendix 1: Functional Compliance Sheet, Sheet Name: AI Security & Guardrails.**

Key Deliverables:

1. End-to-end deployed and operational AI Security & Guardrails solution securing enterprise AI applications, GenAI services, LLMs, AI agents, APIs
2. Centralized management console with real-time dashboards.
3. Configuration and implementation of AI security policies, including prompt injection detection, jailbreak protection, sensitive data masking etc.
4. SOPs, architecture documents, administration guides, operational runbooks, policy documentation, and knowledge transfer/training sessions for Bank personnel covering AI governance, AI Security operations, incident response, policy tuning, and ongoing management of AI Guardrails.

7.4 Bidder Responsibilities

1. Project planning, rollback planning, project governance, and submission of detailed implementation methodology and timelines.
2. The Bidder should note that the Bank is in the process of modernizing and migrating its IT Security ecosystem, and associated security platforms.
3. The Bidder shall ensure that the proposed solution is designed and implemented in a manner that is fully compatible with the Bank's current environment as well as its target security architecture. This shall include, but not be limited to, integration of readiness with existing and future security tools.
4. The Bidder shall be responsible for factoring all required integration, interfacing, API connectivity, log forwarding, and interoperability requirements as part of the overall solution design, sizing, and implementation scope, without any additional cost implications to the Bank.
5. Capacity planning, hardware/software sizing, and bill of materials validation.
6. Security baseline configuration as per industry best practices and security configuration document of the bank.
7. Knowledge transfer sessions and administrator training for Bank IT/Security teams.

8. Coordination with OEMs, third-party vendors, ISPs, and internal stakeholders during implementation and troubleshooting
9. Provide post Go-Live support, stabilization support, and issue resolution during warranty/ATS period
10. Configure monitoring, alerting, dashboards, reporting, and automated notification mechanisms.
11. Support periodic review, perform fine-tuning, patch management, firmware upgrades, and signature/database updates during support period.
12. Maintain audit trails, implementation records, and change management documentation for all activities performed
13. Provide 24x7 technical support escalation matrix and incident response coordination mechanism

7.5 OEM Responsibilities

1. Bidder to note that all the requirements pertaining to Requirement analysis, System design, Development & Installation, Documentation, Deployment and Go-live are to be performed by the respective solution OEM.
2. Respective solution OEM along with the bidder should design High-Level Enterprise Security Architecture that integrates the proposed solution with existing security solutions for both on-premises and cloud environments (Public & private). This architecture should encompass all security components such as perimeter defense, network segmentation, identity and access management, data protection, and threat detection. The design must ensure seamless interoperability between on-premises infrastructure and cloud environments, adhering to industry's best practices and regulatory compliance standards.
3. Assessment of existing system, deployment, configurations, policies and Preparation and submission of High-Level Design (HLD) and Low-Level Design (LLD) documents.
4. Preparation of as-built documentation, configuration documents, SOPs, and operational manuals
5. Integration of the proposed solution with Bank IT & Cyber Security systems like SIEM, two-factor authentication, wireless APs, reporting tools, etc.
6. Configuration/integration for log correlation with standard SIEM tools, SOC Big Data Logs, syslog servers etc.
7. Integration with enterprise authentication systems, including Microsoft Active Directory (AD), RADIUS, and TACACS+ etc. This capability should enable centralized user authentication, role-based access control, and audit logging aligned with organizational identity management policies
8. Configuration of identity-based rules using LDAP/AD/RADIUS/Kerberos integrations and enable granular access controls.
9. Enable/Configure application-based policies, user controls, bandwidth rules, and ensure proper deployment of IPS/IDS capabilities.
10. Ensure compatibility and integration of the proposed solution with the existing IT infrastructure including wired and wireless components.
11. Configuration of the proposed to ensure SSL decryption rule configuration and policy enforcement for encrypted traffic inspection.
12. Perform feasibility study and conduct actual migration of the existing firewalls architecture, configuration, rules, application profile, signatures, policies etc.

13. Develop and Configure Out of the box or custom interfaces to integrate with multiple security monitoring and reporting tools available in the bank's environment such as SIEM, SOAR, APT, and TIP etc.
14. Migration planning, testing, phased rollout, and cutover execution with minimal downtime.
15. Performance tuning, health checks, and system stabilization post deployment.
16. Performing System Integration Testing (SIT), and support during audit/compliance validation
17. Remediation of identified VAPT & Audit gaps related to the Configured solution.
18. Ensure compliance with Bank security policies, regulatory requirements, and applicable industry standards
19. Submission of final acceptance & go-live report and successful handover of the solution to the Bidder's operations team
20. Bidder is also required to factor the highest-level support from the solution OEM during the O&M, warranty, ATS & AMC phase, respective solution OEM is to be involved every year during the O&M phase for performing the configuration, rules and parametrization review along with the solution architecture review at all the environment of PSB.
21. Any requirements from the Bank for customization, enhancement and other device/solution administration-related activity required in the supplied solutions to deliver seamless, fully functional integration, custom and native parsers, connectors, incidents management and related workflows, native and custom playbooks, alerts fine-tuning, notifications, dashboards, reporting, customization of default templates, additional remediation efforts etc. shall be undertaken by the Bidder at no cost to the Bank during the Contract period, even in case of extension of timelines for the commission of IT Security due to any reason and such extension would be at the sole discretion of the Bank
22. The OEMs must provide, maintain and update SBOM, CBOM & AI-BOM as per CERT-IN guidelines including all the dependencies up to the last level.

7.5.1 Migration - Activities are to be performed by Respective solution OEM (supported by bidder)

The bidder and respective proposed product OEM shall coordinate with the Bank and incumbent vendors to ensure seamless migration from the existing solutions to the proposed platform without disruption to business operations. The bidder shall take over all relevant artifacts, documentation, configurations, customizations, software components, manuals, certificates, reports, patches, releases, and other dependencies required for successful migration and transition.

The OEM (assisted by bidder) shall be responsible for migration of all applicable data, configurations, policies, rules, telemetry, logs, parsers, metadata, integrations, and customizations from existing IT and Security solutions to the proposed solutions.

The migration approach shall be applicable across all proposed IT and Cyber Security solutions wherever relevant.

The OEM shall perform all necessary mapping, transformation, parser development/customization, rule migration, configuration alignment, validation, reconciliation, and testing activities required for successful migration and functional equivalence of the proposed solution.

The Respective OEM along with the bidder has to take handover of Data Dictionary, Patches & Releases (If any), Application Software, all content used in the Development of the application, along with Technical Documents, user manual, functional manual, certifications, security certificate and all reports during error correction and installation guide from the existing bank's vendor(s).

Migration of all existing solutions (Existing IT and security solutions to proposed IT Security and other security solutions). Bank currently has an IT Security setup in its co-hosted premises at DC & DR.

The bidder shall develop and submit a comprehensive Migration Plan encompassing, but not limited to, the following key components:

- Current State Assessment
- Migration Strategy and Methodology
- Dependency and Integration Mapping
- Data and Configuration Migration
- Rule, Policy and Parser Migration
- Testing and Validation Approach
- Parallel Run and Cutover Strategy
- Rollback and Recovery Plan
- Risk Assessment and Mitigation
- Resource and Responsibility Matrix
- Migration Timeline and Milestones
- Post-Migration Support and Stabilization Period

The bidder shall be responsible for migrating all applicable data, configurations, and operational components from the existing solution to the proposed platform, including but not limited to:

1. Telemetry Data
2. Historical and Active Logs
3. Rules, Policies, Configurations, and Use Cases
4. Existing Customizations and Workflows
5. Parsers, Connectors, and Integrations
6. Metadata and Contextual Information
7. Dashboards, Reports, and Alerts
8. Asset Inventory and Discovery Data
9. User Profiles, Roles, and Access Configurations
10. Associated Configurations
11. Any other data, configurations, components, or operational elements necessary to ensure a complete, successful, and seamless migration of the existing solution to the proposed platform.

The Detailed Migration Plan shall, at a minimum, cover the following areas:

1. Migration Strategy, Schedule, Tasks, and Activities
2. Resource Requirements (Hardware, Software, Personnel, Facilities, and Other Resources)

3. Dependencies and Interfaces with Other Bank Teams, Applications, and Projects
4. Governance, Management Controls, and Escalation Mechanisms
5. Progress Monitoring and Reporting Procedures
6. Risk, Issue, Dependency, Contingency, and Rollback Management
7. Transition Team Structure, Roles, and Responsibilities
8. Transition Impact Assessment and Business Continuity Considerations
9. Review, Validation, Testing, and Sign-off Processes
10. Configuration, Version, and Change Control Procedures
11. Migration Acceptance and Approval Process
12. Tools, Methodologies, Automation Frameworks, and Technical Capabilities to be utilized for migration and transition activities.

The bidder and respective OEM shall submit and execute a comprehensive migration framework covering, at a minimum, the following phases and associated activities for the seamless migration of solutions, services, data, logs, configurations, and related components from the Bank's existing environment and incumbent service providers:

Service Requirement	Description
Initiation	Establish migration governance, conduct kick-off meetings, finalize scope, responsibilities, timelines, dependencies, and obtain approval of the migration plan.
Planning	Perform detailed assessment and planning activities required for successful migration, including resource planning, dependency mapping, risk assessment, migration strategy, testing approach, rollback procedures, and transition scheduling.
Execution	Execute migration of solutions, services, data, configurations, logs, integrations, and associated components while ensuring minimal risk, business continuity, data integrity, and no disruption to critical banking operations.
Closure & Stabilization	Complete validation, documentation, knowledge transfer, sign-offs, stabilization activities, MIS and SLA reporting setup, operational handover, and commencement of support and maintenance services for the in-scope solutions and infrastructure.

The bidder and respective OEM shall adhere to the implementation timelines approved by the Bank. In the event of any delay in implementation of the proposed solution, the bidder shall, upon the Bank's direction, undertake the takeover, transition, maintenance, and management of the corresponding existing solutions and services from the incumbent vendor until successful Go-Live of the proposed solution. The bidder shall deploy adequately qualified onsite resources, as approved by the Bank, to maintain service continuity and ensure compliance with the applicable SLAs during the transition period. The

bidder shall be responsible for all activities necessary to operate and support the existing solutions until the proposed solution is commissioned and accepted by the Bank.

The manpower deployed for maintenance and management of the existing solutions shall be paid on actual deployment basis, subject to Bank approval and acceptance, at the rates quoted by the bidder for L1, L2, L3 resources and Project Manager in the Year-1 Bill of Material. Such deployment shall commence immediately upon breach of the implementation timelines applicable to the respective solution.

The Bank shall not be liable to pay any costs, fees, or charges towards Annual Technical Support (ATS) or Annual Maintenance Contract (AMC) pertaining to the existing solutions and services. All such costs shall be borne solely by Bidder without recourse to the Bank.

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

1. The respective Solution OEM, assisted by the bidder, shall conduct a detailed assessment of the Bank's business, functional, technical, operational, security, compliance, and integration requirements and design a scalable, resilient, and future-ready solution. The proposed solution shall fully comply with the requirements specified in the RFP and support future business and technology needs of the Bank.
2. As part of the requirement gathering phase, the OEM shall conduct workshops, discovery sessions, interviews, and discussions with the Bank's stakeholders and appointed consultants to understand business requirements, existing infrastructure & solutions, integrations, operational processes, and security requirements.
3. The OEM shall review the Bank's existing IT, security, application, network, cloud, and infrastructure landscape and recommend an optimized target-state architecture leveraging both existing and proposed components wherever feasible.
4. The OEM shall identify all required data sources, integrations, dependencies, interfaces, telemetry sources, and compliance requirements and prepare a detailed solution architecture and deployment design in consultation with the Bank.
5. The scope shall include, but not be limited to:
 - a. Requirements elicitation and analysis
 - b. Gap assessment and solution mapping
 - c. Leveraging standard product capabilities, policies, rules, parsers, controls, and automation features
 - d. Identification of functional, technical, operational, security, reporting, and integration requirements
 - e. Definition of data sources, use cases, workflows, dashboards, reports, and analytics requirements
6. The bidder and OEM shall coordinate with the Bank's internal teams, existing vendors, OEMs, and service providers to gather information required for integration, migration, deployment,

and operationalization of the proposed solution. The Bank shall facilitate necessary coordination wherever required.

7. The bidder and OEM shall prepare and submit a Functional Requirement Specification Manual (FRSM) covering all agreed functional, technical, integration, reporting, operational, security, and compliance requirements. The FRSM shall be reviewed by the Bank, and any observations or approved additions shall be incorporated prior to finalization.
8. The bidder and OEM shall implement and deliver all functionalities, integrations, software, hardware, licenses, infrastructure components, and services required to meet the requirements defined in the approved FRSM, RFP, and associated project documents.

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

1. The bidder and respective OEM shall be responsible for the end-to-end design, sizing, customization, configuration, integration, implementation, deployment, maintenance, and support of the proposed solution, including coordination with all associated OEMs, service providers, and stakeholders.
2. All proposed IT Security solutions shall support seamless interoperability, real-time integration, event sharing, correlation, orchestration, and automated response capabilities to enable unified security operations and minimize manual intervention.
3. The proposed solution shall be configurable and customizable to meet the Bank's functional, technical, operational, reporting, security, and compliance requirements.
4. The bidder and OEM shall design and implement a secure, scalable, resilient, and future-ready architecture based on the approved requirements, data flows, integrations, and operational needs of the Bank.
5. The bidder and OEM shall prepare and submit the following design documents for Bank approval:
 - a. High-Level Design (HLD), including solution architecture, deployment architecture, integration architecture, and data flow architecture.
 - b. Low-Level Design (LLD), including detailed technical specifications, interface specifications, deployment details, configuration standards, and integration mechanisms.
 - c. Technical architecture documentation covering processes, interfaces, deployments, data flows, transformations, reporting, security controls, and operational workflows.
6. The bidder and OEM shall be responsible for implementation of all solution components, integrations, interfaces, workflows, automation, business rules, exception handling, logging, monitoring, archival mechanisms, data exchanges, deployment activities, and testing required for successful commissioning of the solution.
7. The bidder and OEM shall ensure seamless integration with the Bank's internal systems, external entities, regulatory interfaces, fintech partners, and third-party applications through standards-based and scalable integration mechanisms, enabling future expansion through a plug-and-play model.
8. The bidder shall remain fully accountable for successful end-to-end solution delivery and achievement of all functional, technical, operational, performance, security, and compliance requirements specified in the RFP.

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

1. All installation, configuration, customization, testing, migration, integration, UAT, Go-Live, and related implementation activities shall be performed from the Bank's premises. Remote access or VPN access shall not be provided unless explicitly approved by the Bank during unavoidable situations.
2. The bidder and respective OEM shall integrate the proposed solution with the Bank's ITSM, SLA Monitoring, monitoring, logging, authentication, and other enterprise platforms, as required.
3. The bidder and OEM shall coordinate with all relevant third parties, OEMs, service providers, and Bank stakeholders to ensure seamless integration, interoperability, and end-to-end functionality of the proposed solution.
4. The bidder shall provide all required integrations, connectors, parsers, APIs, workflows, playbooks, dashboards, reports, alerts, fine-tuning, customizations, enhancements, and remediation activities necessary for successful operation of the solution throughout the contract period without any additional cost to the Bank.
5. The bidder shall adopt and submit an implementation methodology covering solution deployment, customization, testing, managed services, facility management services, knowledge transfer, and hardware/software installation and configuration activities.
6. The proposed solution shall be complete in all respects and shall not require any additional third-party software, licenses, tools, or components beyond those proposed under this RFP. Any such dependencies shall be identified, supplied, implemented, and commercially included by the bidder.
7. The solution and associated services shall comply with applicable regulatory, statutory, and industry standards, including RBI guidelines, DPDP requirements, Government of India directives, PCI-DSS, ISO standards, and other applicable compliance requirements.
8. The implementation approach shall clearly define inputs, activities, outputs, deliverables, tools, templates, timelines, review mechanisms, and sign-off procedures for each phase of the project.
9. The bidder shall adhere to established quality management, project governance, and risk management practices and shall provide the necessary templates, processes, and controls for effective project execution.
10. The implementation scope shall include requirement gathering, SRS/FRS preparation, customization, installation, configuration, integration, testing, migration, cutover, Go-Live, stabilization, and knowledge transfer activities.
11. The bidder shall ensure active participation of its personnel and OEM resources throughout the implementation lifecycle to facilitate effective knowledge transfer and operational readiness of the Bank's teams.
12. The bidder shall size, provision, implement, and support the required IT infrastructure in accordance with the RFP requirements. Any shortfall in sizing, capacity, performance, availability, or scalability identified during implementation or the contract period shall be rectified by the bidder at no additional cost to the Bank.

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

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

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

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

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

1. The bidder and respective OEM shall be responsible for deployment of the solution in the production environment, Go-Live planning, implementation, installation, configuration, fine-tuning, migration, stabilization, and hyper care support.
2. The bidder and OEM shall provide onsite support during the hyper care period, monitor solution performance, assist users, conduct training sessions, address issues and defects, implement corrective actions, and recommend operational best practices.
3. The implementation scope shall include deployment planning, migration, testing, validation, issue resolution, user acceptance support, Go-Live execution, and post-Go-Live stabilization activities.
4. Prior to Go-Live, the solution shall undergo security validation activities, including VAPT, IS Audit, readiness assessments, identification of security gaps and blind spots, risk remediation, and implementation of recommendations. The Bank or its appointed agency may conduct Red

Teaming, Purple Teaming, security assessments, or other validation exercises as deemed necessary.

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

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

1. The Bank shall conduct User Acceptance Testing (UAT) to validate that the proposed solution and all associated components, integrations, workflows, reports, dashboards, and functionalities comply with the requirements specified in the RFP, approved FRSM/SRS, and other project documents.
2. The bidder and respective OEM shall confirm completion of all implementations, configuration, customization, integration, migration, and testing activities prior to commencement of UAT and certify that the solution is ready for user validation.
3. The bidder shall provision and maintain dedicated Development, Testing, UAT, and Pre-Production environments throughout the contract period. All software, licenses, and other resources required for such environments shall be included within the bidder's scope without any additional cost to the Bank.
4. Any defects, deviations, vulnerabilities, observations, or non-compliances identified during UAT, security assessments, audits, reviews, or validation exercises shall be rectified by the bidder within the timelines prescribed by the Bank and at no additional cost.
5. The bidder shall maintain appropriate version control, configuration management, change management, release management, and documentation controls throughout the implementation and testing lifecycle.

6. The bidder shall update all technical, operational, security, user, and administrative documentation to reflect changes, enhancements, configurations, fixes, and upgrades implemented during the project.
7. The bidder shall remediate security vulnerabilities, gaps, weaknesses, audit observations, and control deficiencies identified during implementation, testing, assessments, audits, reviews, or operational activities, subject to Bank approval wherever required.
8. During the contract period, the bidder shall support periodic reviews, assessments, audits, and compliance validation activities, as required by the Bank, including but not limited to:
 - Policies, procedures, and governance controls
 - IT General Controls (ITGC)
 - Logical Access Management and Privileged Access Management
 - Physical and Environmental Security Controls
 - Change and Release Management Processes
 - Third-Party and Vendor Management Controls
 - Backup, Recovery, and Data Protection Controls
 - Incident Management Processes
 - Business Continuity and Disaster Recovery Arrangements
 - Security Configurations and Hardening Standards
 - Operating Systems, Databases, Applications, Network Devices, Security Devices, and Cloud Infrastructure Security Reviews
9. The bidder shall provide all necessary support, documentation, evidence, reports, logs, and resources required for successful completion of such reviews, assessments, audits, and compliance activities.

7.7.6.1 Quality Assurance

1. Testing Requirements

- a. The respective OEM shall be responsible for planning, executing, documenting, and successfully completing all testing activities required to validate the functionality, performance, stability, reliability, security, interoperability, and operational readiness of the proposed solution. The bidder shall prepare detailed test plans, test cases, test data, automation scripts (where applicable), entry and exit criteria, test reports, defect logs, root cause analysis reports, workarounds, and remediation plans, and shall obtain the Bank's approval wherever required.

2. Test Preparation

The respective OEM shall:

- a. Prepare the overall testing strategy and methodology for Unit Testing (UT), System Integration Testing (SIT), UAT, Performance Testing, Security Testing, and other applicable tests.
- b. Establish and maintain the required test environments, infrastructure, software, applications, and test data.

- c. Prepare, validate, and execute test cases, scripts, and automation frameworks, wherever applicable.
- d. Define test entry and exit criteria, acceptance criteria, and success parameters.

3. Test Execution

The respective OEM shall:

- a. Execute all approved test cases and scripts.
- b. Record, track, report, and resolve defects, deviations, and observations.
- c. Perform re-testing and regression testing after issue resolution.
- d. Submit test results, defect reports, execution evidence, and test summary reports in formats approved by the Bank.
- e. Provide recommendations for usability, performance improvements, operational enhancements, and risk mitigation.

4. Types of Testing

The respective OEM shall perform, at a minimum, the following testing activities, wherever applicable:

- a. Unit Testing (UT)
- b. System Integration Testing (SIT)
- c. User Acceptance Testing (UAT) Support
- d. Functional Testing
- e. Performance, Load, Stress, Volume, and Scalability Testing
- f. Security and Configuration Validation Testing
- g. Data Migration Testing
- h. Interface and Integration Testing
- i. Compatibility and Interoperability Testing
- j. Exception Handling and Failover Testing
- k. Installation and Upgrade Testing
- l. Regression and Sanity Testing
- m. Operational Readiness Testing
- n. Usability Testing
- o. Any other testing required to ensure successful implementation and acceptance of the solution
- p. The bidder & OEM shall rectify all defects, vulnerabilities, configuration issues, integration issues, performance bottlenecks, and non-compliances identified during testing at no additional cost to the Bank. Successful completion of all testing activities and closure of observations shall be a prerequisite for progression to subsequent project phases and Go-Live approval.

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

The bidder and respective OEMs shall provide comprehensive product training, knowledge transfer, and certification programs for the Bank's IT and Information Security personnel at no additional cost. All technical and product-specific training shall be delivered by OEM. Upon successful completion of the

training programs, the respective OEM shall issue participation and/or certification certificates to the attendees.

The bidder shall submit a detailed Training and Certification Plan covering training objectives, curriculum, skill levels, training schedules, participant eligibility, certification pathways, and assessment criteria. The training program shall cover product functionalities, administration, troubleshooting, maintenance, security best practices, automation, advanced threat scenarios, new features, upgrades, operational workflows, and industry trends.

At a minimum, the following training programs shall be conducted for each proposed solution/OEM:

Training Type	Duration per Session	Minimum Number of Sessions
Beginner / Foundation Training	2 Days	5 Sessions
Advanced / Administrator Training	3 Days	5 Sessions
Backend Administration, Troubleshooting & Maintenance Training	3 Days	5 Sessions

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

7.5.9 Security requirements - Activities are to be performed by Respective solution OEM (supported by bidder)

1. The bidder and respective OEMs shall comply with the Bank's IT, Information Security, Cyber Security, Data Protection, Privacy, Business Continuity, and related policies, standards, procedures, and guidelines, as shared by the Bank from time to time. The bidder shall be responsible for ensuring the confidentiality, integrity, availability, security, and privacy of the Bank's information assets, systems, applications, and data throughout the contract period.
2. The bidder shall implement and maintain appropriate administrative, technical, physical, and operational controls for protection of data, applications, systems, infrastructure, and associated assets under its custody or management.
3. The bidder shall comply with the Bank's requirements relating to access management, privileged access management, password policies, user administration, data protection, encryption, monitoring, incident management, and security governance.
4. The bidder shall ensure encryption and protection of data at rest, data in transit, and data in use, wherever applicable, using industry-standard security controls and cryptographic mechanisms. All tools, technologies, and controls required to achieve the same shall form part of the proposed solution.
5. The bidder and OEM shall comply with all applicable regulatory, statutory, legal, and industry requirements, including RBI & GOI guidelines, DPDP Act, NCIIPC guidelines, CERT-In advisories, and other applicable cybersecurity and data protection requirements.
6. All Bank data, including production data, backup data, logs, telemetry, monitoring information, license-related data, and any other information generated, processed, transmitted, or stored by the

proposed solution, shall reside within India. No Bank data shall be transmitted, replicated, processed, accessed, stored, or exchanged outside India without prior written approval from the Bank and applicable regulatory permissions.

7. The bidder shall ensure that Personally Identifiable Information (PII), sensitive personal data, financial information, and other confidential information are appropriately masked, encrypted, protected, and accessible strictly on a need-to-know basis in accordance with the Bank's access control policies.
8. The bidder shall provide all logs, records, evidence, reports, forensic artifacts, and other information required by the Bank for security investigations, regulatory reviews, audits, incident response activities, and forensic analysis.
9. The bidder shall promptly report information security incidents, cyber incidents, breaches, vulnerabilities, and control failures affecting the proposed solution and shall provide detailed incident reports, root cause analysis, corrective actions, and preventive measures.
10. The bidder and OEM shall establish, implement, and maintain secure baseline configurations and hardening standards for all operating systems, databases, applications, network devices, security devices, middleware, cloud resources, and supporting infrastructure and shall periodically review and update the same in accordance with industry best practices and bank's hardening policy.
11. The Bank or its authorized representatives shall have the right to conduct audits, reviews, assessments, inspections, and compliance validation activities relating to the proposed solution, associated processes, controls, facilities, personnel, documentation, and supporting infrastructure. The bidder shall provide all necessary cooperation, access, information, records, and assistance required for such activities.

7.6 Cloud Service Provider Responsibilities

The requirements contained in this section apply to all cloud-hosted solutions proposed under IaaS, PaaS, or SaaS delivery models.

However, the bidder and OEM shall remain fully accountable to the Bank for compliance with all contractual, security, operational, regulatory, and performance requirements specified in this RFP.

1. The bidder/OEM shall establish and manage a dedicated cloud landing zone, including Development, UAT, and Production environments, with appropriate segregation, governance, access controls, monitoring, and SDLC controls.
2. The bidder/OEM shall be responsible for provisioning, configuration, administration, monitoring, patching, upgrading, backup, recovery, migration, and lifecycle management of all cloud resources, including compute, storage, databases, containers, networking, security services, and associated cloud components.
3. The solution shall support secure connectivity with the Bank's on-premises infrastructure, cloud environments, and external systems through private and secure communication mechanisms.
4. The bidder shall ensure compliance with applicable RBI guidelines, DPDP requirements, NCIIPC guidelines, CERT-In advisories, Government of India regulations, Bank policies, and other applicable regulatory, statutory, and industry standards. Necessary compliance artefacts, audit

evidence, risk assessments, reports, and documentation shall be maintained and provided to the Bank as required by bidder/OEM on regular basis as well as whenever required.

5. All Bank data, including production data, backups, logs, telemetry, prompts, metadata, and related information, shall reside within India. No data shall be transmitted, processed, stored, validated, replicated, or accessed outside India without prior written approval from the Bank and applicable regulatory authorities.
6. The bidder and OEM shall provide complete data ownership, data sovereignty, confidentiality, and privacy of the Bank's information. Bank data shall not be used for model training, model retraining, analytics, or shared with third parties, whatsoever, except as explicitly authorized by the Bank in writing.
7. The solution shall support encryption of data at rest, motion, and in transit using industry-standard cryptographic controls and shall support key management through CSP-native KMS and/or the Bank's Key Management System.
8. The CSP environment shall provide comprehensive monitoring, logging, audit trails, governance controls, compliance reporting, security event monitoring, and forensic investigation capabilities through centralized dashboards and reporting mechanisms to the bank.
9. The cloud platform shall support high availability, fault tolerance, disaster recovery, multi-site deployment, backup and recovery services, and business continuity capabilities in accordance with the Bank's RTO, RPO, availability, and resilience requirements.
10. The CSP shall provide enterprise-grade support services, including 24x7 support, incident management, escalation management, defined service levels, and proactive operational support throughout the contract period.
11. The bidder shall be responsible for sizing all cloud resources, including compute, containers, databases, storage, caching, networking, API gateways, load balancers, egress/ingress and related services. Any capacity shortfall affecting performance, scalability, availability, or SLA compliance shall be addressed by the bidder at no additional cost to the Bank.
12. The bidder shall provide periodic utilization, performance, capacity, availability, security, backup, and SLA compliance reports for all cloud-hosted services as per the reporting requirements defined in the RFP.
13. The cloud platform shall provide native audit logging, security monitoring, vulnerability management, backup management, access management, and security controls necessary for secure operation of the proposed solution throughout the contract period.
14. If, at any time during the contract period or during any audit, assessment, review, inspection, or compliance validation exercise, any deviation, non-compliance, deficiency, or control gap is identified, the bidder shall promptly rectify the same within the timeline prescribed by the Bank. Until such deviation or non-compliance is fully remediated and accepted by the Bank, the bidder shall remain liable for applicable penalties, and other contractual remedies as specified in the RFP and contract.
15. The bidder shall submit compliance against the Technical Specifications – Sheet Name: CSP Compliance Requirements for every solution proposed under IaaS, PaaS, or SaaS deployment models. The compliance shall clearly demonstrate that the proposed cloud environment,

associated services, and all supporting components, including the proposed solution, fully meet the technical, security, operational, regulatory, and contractual requirements specified in this RFP.

The bidder shall submit a consolidated compliance declaration on its own official letterhead for every cloud-hosted solution proposed under this RFP. The declaration shall clearly specify:

- a. Name of the proposed Solution OEM.
- b. Name of the Cloud Service Provider (CSP)
- c. Deployment model (IaaS, PaaS, or SaaS).
- d. Cloud hosting location(s), cloud region(s), and data residency details.
- e. Roles and responsibilities of the bidder, Solution OEM, and CSP for implementation, operations, security, monitoring, support, backup, disaster recovery, compliance, and SLA management.
- f. Confirmation that there are no gaps in ownership or accountability between the bidder, OEM, and CSP for any obligation defined in this RFP.
- g. The bidder shall ensure that the submitted compliance clearly identifies the Solution OEM, CSP, deployment model (IaaS/PaaS/SaaS), cloud region(s), hosting location(s), and the roles and responsibilities of each party for delivering and supporting the proposed solution, the same is to be submitted on bidder's letterhead for all the solution proposed on Cloud.

Cloud Deployment Model

a. IaaS and/or PaaS Deployment Model:

For solutions proposed under Infrastructure as a Service (IaaS) and/or Platform as a Service (PaaS) deployment models, the compliance (**Functional Specification Sheet: CSP Compliance Requirements**) shall be submitted on the official letterhead of the respective Cloud Service Provider (CSP) and shall be duly signed and stamped by the authorized representative of the CSP. The compliance shall confirm that CSP's cloud infrastructure and managed cloud services fully comply with the requirements specified in this RFP.

b. SaaS Deployment Model:

For solution proposed under the Software as a Service (SaaS) deployment model, the following requirements shall be applicable:

1. Compliance against the **Functional Specification Sheet: CSP Compliance Requirements** shall be submitted on the official letterhead of the Proposed Solution OEM, duly signed and stamped on by its authorized representative.
2. The Solution OEM shall submit the complete compliance against the Technical Specifications – Sheet Name: CSP Compliance Requirements on its official letterhead, duly signed and stamped by its authorized representative. The Solution OEM shall provide compliance against each, and every requirement specified in the CSP Compliance Requirements Sheet and shall not leave any requirement unanswered.

3. Where the SaaS solution is hosted on a third-party cloud platform, the Solution OEM shall ensure that the underlying CSP infrastructure also complies with all applicable CSP requirements defined in this RFP. The Solution OEM shall obtain the necessary compliance confirmation from the CSP and shall remain responsible for ensuring such compliance throughout the contract period. The SaaS Solution shall submit compliance for each and every CSP Compliance Requirement on their letterhead.

7.7 Non-functional requirements

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

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

7.8 Delivery, Installation & Commissioning

1. The bidder shall ensure appropriate packaging, handling, transportation, and delivery of all required hardware, software, appliances, and associated components to prevent damage,

deterioration, or loss during transit and storage. All products should be brand new and shall be supplied in original OEM packaging & factory-sealed condition.

2. Delivery, installation, configuration, integration, testing, commissioning, and operationalization of the proposed solution shall be completed at the designated Bank locations within the timelines specified in the RFP and approved project plan.
3. Delivery shall be deemed complete upon receipt of all ordered products, components, licenses, software, firmware, documentation, and associated materials at the designated Bank location(s) in good condition.
4. Installation and commissioning shall be deemed complete only upon successful deployment, configuration, integration, testing, and demonstration of all functionalities, features, and performance requirements specified in the RFP to the satisfaction of the Bank.
5. The bidder shall rectify any defects, deficiencies, performance issues, integration issues, or non-compliances identified during installation, commissioning, testing, acceptance, or operationalization at no additional cost to the Bank.
6. The bidder shall provide all relevant documentation, including invoices, delivery acknowledgements, packing lists, warranty certificates, insurance documents, licenses, technical manuals, installation guides, operational manuals, and other documents required by the Bank.
7. All software, firmware, licenses, subscriptions, and related components supplied under the contract shall be genuine, legally procured, appropriately licensed, and fully supported by the respective OEMs throughout the contract period. The bidder shall provide documentary evidence of OEM authorization, licensing rights, and support arrangements wherever applicable.
8. Final acceptance of the solution shall be subject to successful completion of installation, integration, testing, commissioning, acceptance testing, and sign-off by the Bank. If any component fails to meet the requirements specified in the RFP, the bidder shall undertake necessary rectification, replacement, upgrade, or augmentation at no additional cost to the Bank.
9. Ownership of all supplied hardware, software licenses, associated entitlements, and other assets purchased under this RFP shall vest with the Bank upon delivery and acceptance. The bidder shall provide all necessary documents, certificates, and evidence establishing the Bank's ownership and perpetual usage rights, wherever applicable, prior to release of payment.

7.9 Data Privacy

Data Privacy and Confidentiality

1. The bidder and respective OEMs shall ensure that no Bank data, information, logs, reports, configurations, intellectual property, or other artifacts are copied, transmitted, transferred, stored, processed, published, or accessed outside the Bank's authorized environment without prior written approval from the Bank.
2. The bidder and OEMs shall maintain strict confidentiality of all Bank information during and after the contract period and shall ensure that no Bank information is disclosed, published, shared, or used for any purpose other than performance of the services under this RFP.

3. The bidder and OEMs shall comply with the Bank's IT, Information Security, Cyber Security, Data Governance, Privacy, Data Retention, DPDP, and other applicable regulatory, statutory, and contractual requirements.
4. All data, information, records, logs, metadata, configurations, policies, rules, reports, security events, transaction information, customer information, credentials, encryption keys, certificates and other information generated, collected, processed, stored or accessed in connection with the services shall remain the exclusive property of the Bank. The Vendor shall acquire no right, title, interest, lien or licence therein except the limited right to process such information strictly for performance of the Contract.
5. The Bidder shall not transfer, host, process, mirror, replicate or permit access to Bank Data outside India without the prior written approval of the Bank and subject to applicable law, regulatory directions and Bank policy. No Bank Data shall be transferred to any offshore location, cloud environment or third-party repository without prior written approval of the Bank.
6. The Bidder shall comply with all applicable data protection, privacy, cyber-security and information-security laws, rules, regulations, directions and regulatory instructions applicable to the Bank and/or the services, as amended from time to time.

Executive Governance and Project Oversight

1. The bidder and each respective OEM shall nominate a senior executive as Project Sponsor / Project Director for the engagement. Such personnel shall be responsible for executive governance, strategic oversight, stakeholder management, escalation management, and overall success of the project.
2. The Project Sponsor / Project Director and other designated senior executives shall participate in governance meetings, executive reviews, strategy workshops, presentations, and brainstorming sessions with the Bank as and when required. At a minimum, quarterly executive review meetings shall be conducted throughout the contract period or at regular intervals as per Bank's discretion.
3. The bidder and OEMs shall ensure deployment of adequately skilled, certified, experienced, and qualified resources required to meet the scope, service levels, functional requirements, technical requirements, and operational objectives defined in the RFP.
4. The bidder shall establish and maintain Key Performance Indicators (KPIs), Key Risk Indicators (KRIs), operational metrics, and governance dashboards for continuous monitoring of service quality, performance, security, compliance, risk, and operational effectiveness.
5. The bidder shall establish a Governance, Risk and Compliance (GRC) framework for the proposed solution and obtain the Bank's approval for the same within the timelines prescribed by the Bank.
6. Senior representatives of the bidder and OEMs shall periodically engage with the Bank to review project progress, service delivery, operational performance, automation opportunities, technology enhancements, security posture, compliance requirements, and industry best practices, and provide recommendations for continuous improvement.
7. The bidder shall support the Bank's IT, Information Security, Cyber Security, compliance, audit, governance, and transformation initiatives related to the scope of this RFP.

8. The bidder shall ensure adequate staffing, succession planning, backup resources, and skill development mechanisms to support uninterrupted 24x7x365 operations throughout the contract period.
9. The bidder shall ensure that all onsite resources receive appropriate training on the deployed technologies, operational procedures, troubleshooting, administration, security operations, threat management, risk management, automation, analytics, and other relevant functions.
10. The Bank reserves the right to review the performance, competency, conduct, and suitability of the bidder's and OEM's personnel. Any resource found unsuitable, underperforming, or non-compliant with the Bank's requirements shall be replaced by the bidder with an equivalent or better-qualified resource within the timeline prescribed by the Bank.

7.10 Solution/Appliance Warranty, ATS and AMC

1. The bidder shall quote Annual Technical Support (ATS) and Annual Maintenance Contract (AMC) charges separately for the period commencing after the expiry of the warranty period. The proposed solution, hardware/appliances and software shall include a comprehensive warranty for a period of three (3) years.
2. Bidder needs to provide the comprehensive ATS & AMC separately for Year 4 and Year 5.
3. Warranty period for hardware/appliance and software support shall commence from the date of Go-live of the respective solution.
4. The bidder shall provide comprehensive onsite warranty, AMC for all proposed hardware components and comprehensive ATS/subscription support for all software, licenses, subscriptions, and services supplied under this RFP for the entire contract period.
5. Warranty, AMC and ATS services shall include OEM support, software updates, upgrades, patches, bug fixes, technical assistance, preventive maintenance, corrective maintenance, replacement of defective components, security updates, and all other activities required to ensure continuous and secure operation of the solution.
6. All Warranty, AMC and ATS services shall comply with the technical standards, security requirements, operating procedures, business continuity requirements, and recovery procedures specified in the RFP and applicable Bank policies.
7. The rates quoted by the bidder for hardware, software, subscriptions, licenses, ATS, AMC, and related services shall be applicable on a pro-rata basis for any additional quantities or services procured by the Bank during the contract period.
8. Installation of supplemental hardware by the Bank, with due intimation to the bidder and OEM, shall not invalidate or adversely impact the OEM Warranty, ATS, or AMC coverage of the originally supplied hardware. However, Warranty, AMC and ATS obligations shall not extend to such supplemental hardware unless specifically procured under this contract.

7.11 Resource Requirement

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

Implementation Phase:

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

Operations and Maintenance (O&M) Phase:

The bidder shall deploy the minimum onsite L1, L2, Project Manager – Operations, and other resources as specified in the RFP and ensure 24x7x365 support coverage through an appropriate shift-based deployment model.

The respective OEMs shall provide L3 support resources and subject matter experts from the date of installation and throughout the contract period to support operations, troubleshooting, optimization, upgrades, audits, and major incidents.

The bidder shall ensure adequate onsite and offsite SME support to assist deployed resources and ensure timely resolution of incidents, service requests, problems, vulnerabilities, and operational issues.

Resource Management and Governance

The Bank reserves the right to interview, evaluate, approve, reject, or seek replacement of any proposed resource before or during the contract period. Any resource found unsuitable, underperforming, non-compliant, or lacking the required competencies shall be replaced by the bidder within the timeline prescribed by the Bank.

All deployed resources shall be named resources. Any replacement, withdrawal, reassignment, or removal of resources shall require prior written approval from the Bank.

The bidder shall ensure adequate backup resources, succession planning, cross-training, and knowledge management practices to eliminate single points of dependency and ensure uninterrupted service delivery.

The following minimum transition and knowledge transfer periods shall be adhered to in case of resource replacement:

- Project Manager: 60 Days
- Key Personnel: 45 Days
- Other Personnel: 30 Days

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

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

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

#	Resource Type	Deployment	Minimum Qualification & Experience
Implementation Phase			
1	Project Manager – Implementation	Onsite – as per Bank's timings/ Shift Timings (Full Time)	- Graduate/B.E./B.Tech/MCA with PMP/PRINCE2 or equivalent certification. - Minimum 8 years of experience - Proven experience in managing at least two Security Solution implementations (including at least one Perimeter Security solution) in PSU/PSE/Government/BFSI/Regulatory organizations.
2	OEM Implementation Resources	Onsite – as per Bank's timings/ Shift Timings (Full Time)	OEM shall submit a detailed resource deployment plan before commencement of requirement gathering. Any replacement or modification shall require prior Bank approval.
3	Bidder Implementation Resources	Onsite – as per Bank's timings/ Shift Timings (Full Time)	Bidder shall submit a detailed resource deployment plan before commencement of requirement gathering. Any replacement or modification shall require prior Bank approval.
Operations & Maintenance (O&M) Phase			
4	L1 Security Resources	Onsite – as per Bank's timings/ Shift Timings (Full Time)	- Graduate/B.E./B.Tech/MCA with minimum 2 years of experience. - Minimum one OEM security certifications or equivalent certifications such as CEH, Security+, etc. - Experience in managing at least one IT Security solution in PSU/PSE/Government/BFSI/Regulatory organizations.
5	L2 Security Resources	Onsite – as per Bank's timings/ Shift	- Graduate/B.E./B.Tech. /MCA with minimum 5 years of experience. - Minimum two OEM security certifications or equivalent certifications such as CEH, CISA, etc.

#	Resource Type	Deployment	Minimum Qualification & Experience
		Timings (Full Time)	Experience in managing at least one IT Security solution in PSU/PSE/Government/BFSI/Regulatory organizations.
6	L3/ Project Manager – Operations	Onsite – as per Bank's timings/ Shift Timings (Full Time)	- Graduate/B.E./B.Tech. /MCA with PMP/PRINCE2 or equivalent certification. - Minimum 8 years of experience in IT Security operations and management. - Experience in managing at least three IT Security solution implementation and/or operations engagements in PSU/PSE/ Government/BFSI/ Regulatory organizations.
IT Infrastructure Resources			
7	L1 IT Infrastructure Resources	Onsite – as per Bank's timings / Shift Timings (Full Time)	- Graduate or equivalent. - Minimum 2 years of experience in IT Infrastructure operations. - Experience in managing at least one IT Infrastructure solution in PSU/PSE/Government/BFSI/Regulatory organizations.
8	L2 IT Infrastructure Resources	Onsite – as per Bank's timings / Shift Timings (Full Time)	- Graduate or equivalent. - Minimum 3 years of experience in IT Infrastructure operations. Experience in managing at least two IT Infrastructure solution in PSU/PSE/Government/BFSI/Regulatory organizations.

Note: No remote access shall be provided to any resource

The bidder is required to provide onsite human resource for L1, L2 & L3 resources and respective OEMs are required to provide L3 resource each from the date of IT Security solutions installation. The Bank may be required to increase onsite personnel resources of the bidder and / or OEMs from time to time. The same need to be provided within one month from the date of such communication. The onsite resources must be provided adequate guidance, assistance and support by competent offsite subject matter experts (SME) of the bidder & OEMs

MINIMUM RESOURCE COUNT DEPLOYMENT

The following table represents the minimum onsite resource deployment requirements. The bidder shall right-size and deploy additional L1, L2, L3, OEM, SME, and specialist resources as required to meet the SLA, operational, security, and business requirements defined in the RFP.

#	Shifts	L1 Security (Minimum)	L2 Security (Minimum)	L3/ Project Manager (Minimum)	IT Infrastructure L1 (Minimum)	IT Infrastructure L2 (Minimum)
1	Shift A	3	3	1	1	1
2	Shift B	2	3	Bidder to right size	1	1
3	Shift C	2	2	Bidder to right size	1	1

The Bidder shall ensure that the L1 and L2 security resources deployed in each shift are collectively capable of handling the security domains specified above. Resources may be cross-skilled and mapped to multiple security domains, provided that such arrangement does not affect the required monitoring, incident response, troubleshooting, service levels or operational coverage.

The Bidder shall provide appropriately qualified SMEs for the respective technology domains. SME resources may be shared across domains and shifts, subject to the Bank's service-level requirements. The Bidder shall ensure that the deployed resources collectively possess adequate technical skills and experience across all the following security domains:

#	Security Domain	Minimum Competency Coverage
A	Perimeter & Network Security	Anti-DDoS, SSL/TLS Interception, Network Packet Broker, DNS Protection, Secure Web Gateway, Zero-Day Protection and Zero Trust Network Access
B	Endpoint & Cloud Security	CASB, DLP and DRM
C	Data Security	Database Activity Monitoring, Database Security and Mobile Application Security
D	Application Security	1. Application Security : HIPS, WAF 2. Cryptographic & Software Supply Chain Security : Centralized Key Management, Certificate Lifecycle Management, SBOM, CBOM, AIBOM and QBOM
E	Management Layer Security	1. Identity & Access Security : IDAM, MFA and PIM/PAM, DNS Security Services 2. AI Security: AI Gateway, AI Firewall, AI Guardrails, Prompt Security, AI Governance and AI Data Protection 3. Security Integration & Governance : SIEM/SOC integration, SOAR integration, incident management, security reporting, dashboards and cross-domain security integration

Bidder to factor in the resources with expertise in the security layers as per the following table:

Security Layer	Solutions	Shift A – L1	Shift A – L2	Shift B – L1	Shift B – L2	Shift C – L1	Shift C – L2	Shift A – L3
Perimeter & Network Security	6	0	0	1	1	1	1	1
Endpoint Security	3	1	1	0	1	0	1	

Data Security	2			0		0		
Application Management Security AND layer	9	1	1	2	2	1	0	
Total	20	3	3	2	3	2	2	1

Note:

- Resources may be shared across technologies within the same domain, provided the minimum deployment requirements and SLA commitments are met.
- The bidder shall ensure availability of OEM L3 specialists, architects, and SMEs for all proposed solutions throughout the contract period as and when required as per the requirements, scope of the RFP, and in line with the SLAs.
- The Bank reserves the right to require dedicated resources for any solution based on operational, security, compliance, or business requirements.
- The bidder shall augment resources at no additional cost wherever required to meet service levels, incident response timelines, project milestones, or operational demands.
- The above deployment represents the minimum onsite staffing requirement and shall not relieve the bidder of its responsibility to provide adequate resources for successful delivery of services.

Resource Deployment, Replacement and Governance

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

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

Responsibilities of Project Manager

The Project Manager shall, at a minimum:

- Lead and govern the implementation, transition, and operational activities under the contract.
- Act as the primary point of contact for the Bank's management and stakeholders.
- Be accountable for successful delivery of the project and achievement of agreed timelines, milestones, and service levels.
- Identify, track, escalate, and resolve project risks, issues, dependencies, and bottlenecks.
- Coordinate with OEMs, service providers, Bank teams, and other stakeholders for successful delivery of services.
- Monitor change management, deployment, migration, testing, and operational readiness activities.
- Drive adoption of industry best practices, governance controls, and continuous improvement initiatives.
- Submit periodic project status reports, governance reports, risk reports, and management updates to the Bank.

7.12 Facilities Management

1. Bidder should manage, monitor, maintain and upgrade all proposed solutions & services on ongoing basis encompassing all deployed hardware/ firmware/ middleware / software components by performing timely backups, continuous health monitoring, on-site and offsite support, troubleshooting, critical functional and performance bug fixes, all major product/feature enhancements within the warranty and AMC charges and as per the SLA defined by the Bank.
2. There should be considerable reduction in MTTD and MTTR for security incidents by leveraging technology's own capabilities and SOAR. All daily routine and standard activities of L1 and L2 to be automated in phased manner from the date of Go-live.
3. Bidder shall be responsible to develop and maintain Standard Operating Procedures (SOP) with respect to day to day operations including but not limited to incident management, reports & dashboards, forensics infrastructure maintenance, install/upgrades, updates, asset Integration, Business Continuity data & configuration backup, restoration, archival, knowledge management, segregation of duties, change management, patch & version management, KPI and KRI to measure performance etc. as per policies of the Bank. Bidder to create and modify SOP as per the requirement of the Bank periodically and from time to time, as applicable. All SOP will be reviewed by the Bank on monthly basis.
4. All onsite personnel resources of the bidder & OEMs should ensure to deliver the services leveraging security technologies as mentioned in the technology details, architecture and Terms & conditions in the bid, RFP, annexure, addendums, clarifications etc. issued by the Bank.
5. Bidder onsite personnel should be carrying out regular patch management, firmware updates, software upgrades, security updates, bug fixes, and configuration management of the deployed solution throughout the contract period. All critical, high-risk, and security-related patches/updates released by the OEM shall be assessed and applied in accordance with the Bank's change management procedures. The bidder shall proactively monitor OEM advisories and vulnerabilities and shall promptly implement necessary corrective actions to mitigate identified security risk.
6. Starting from Go-Live date of the respective security solutions, 7th day of every month: Monthly Security Certificate to be submitted by the Project Manager of the bidder and onsite resources of the OEMs stating:
 - a. "To the best of our knowledge and on the basis of logs, data, information collated by the NextGEN SOC in various systems and analysis thereof by us using NextGEN SOC tools, we confirm that no major information / cyber security incident has happened during the last month. The logs, data, information etc. correlated by us confirms no data or information having been compromised, exfiltrated or any of the systems having been compromised / hacked."
 - b. "All the proposed solutions and services are in good health, optimally configured and running at highest capacity & capabilities to be fully effective."
7. Every technology deployed should transform itself from a purely rule based system to analytics & AI/ML based correlation system for logs, vulnerabilities & threat intelligence together for accurate risks prediction.
8. To ensure efficient utilization and monitoring of proposed solution, optimizing capacity utilization, ensuring quality of data and system performance is maintained optimal, there are no security events omission, misfiring rules, heavy rules and reports etc.

9. L3 personnel resources of OEM are expected to provide guidance to L1 & L2 resources. These resources have to understand daily activities of L1 & L2 resources and automate the same in sprints (phases) to achieve automation.
10. Participate and contribute in every DR drill, cyber security drill, tabletop exercises by the Bank, regulators or any third party.
11. Conduct DR drill of the Security on quarterly interval or as and when required by the Bank. Ensure DC & DR are exact replica of each other in every manner.
12. Develop custom plug-ins, parsers, connectors, agents, adopters for all the systems in the Bank or related to the Bank periodically or as and when needed.
13. Develop the baseline for the level of logs to be enabled across the different components of IT including infrastructure, databases, business applications and devices etc. The log baselines should be in line with global best practices including NIST, SANS etc.
14. Perform monthly gap analysis of current levels of logs enabled in OS, databases, web servers, business applications and devices and entire IT infrastructure & recommend and implement remedial actions.
15. Periodically assess the business requirements and configure the required rules, AI/ML based analytics, self-learning models & processes and generate alerts as per the global best practices and Bank's requirements.
16. Securely preserve and maintain baseline repository of all the rules and models on analytical, self-learning, supervised & unsupervised learning and keep track of any changes / modifications.
17. Create new and customize existing reports, dashboards, rules, queries, user interface in all forms to meet the dynamic requirements of the Bank.
18. Define formats for MIS reporting that includes daily, weekly and monthly or any periodical or adhoc reports, dashboards as per the Bank's requirements.
19. Transfer the knowledge to the Bank's employees about day-to-day operations, system / backend level troubleshooting, dashboarding, creating basic and advanced rules & analytical models, creation and customisation of reports & queries etc.
20. Complete system level frontend and backend management & maintenance related knowledge need to be transferred to the Bank's staff by the bidder's onsite L1 & L2 resources.
21. There should not be disruption or degradation in the Bank's network bandwidth utilization and availability due to excessive log transmission.
22. Conduct periodic health check-up of the proposed systems by respective OEMs, refer section OEM Services & Deployment. The recommendations in the report should be rectified by onsite resources, including resources/professional from respective OEM within a week's time. OEMs to ensure that their respective systems operate efficiently, cohesively without any adverse impact on processing, correlation, alerting, dashboarding etc. as per expectations of the Bank, stipulated in the RFP.
23. Secure configuration baseline should be benchmarked and updated on a periodic basis with standards including SANS, NIST, CIS, Bank's policies, CERT-IN, IDRBT, RBI, NCIIPC guidelines as updated from time to time.
24. Bank provided IT Service Management (ITSM) or any other tool identified from time to time should be used for ticketing system, tracking instructions received from application / asset owners like integration, VA, PT, incident management etc. Instructions / actionable for day-to-day functioning within the team should also be routed through such tool. The entries in the tool should be able to provide jobs / activities completed, pending, pending at whose end etc.

- The performance & turnaround time / efficiency of onsite personnel resource would also be evaluated from the MIS generated from this tool.
25. All deliverables including reports, incidents / alerts, their closure, vulnerabilities reported and closed, dashboards, query optimization, indexing, automation based on AI/ML, backup & recovery activities etc. should undergo Quality Assurance process by L2 & L3 resources of the bidder & respective OEM on ongoing basis. Project Manager should define quality metrics, measurement frequency and reporting periodicity in consultation with the Bank.
 26. Ensure security of proposed setup from cyber-attacks & malwares etc. Any suspicious activity, behaviour of the proposed setup must be immediately taken into consideration and acted upon at the top priority.
 27. For the security of the proposed setup, integrate the complete proposed setup with all the currently deployed tools and those procured from time to time.
 28. For security monitoring of the proposed setup, integrate the complete proposed setup with SIEM, SBDL, DAM, NBA, Packet Capture, SOAR, TI etc. and ensure logs are auto sent to these tools by entire proposed setup on real-time basis on 24x7x365 days basis. These tools should automatically & immediately raise the alert to the designated official of the Bank, if no log is received for in 15 minutes initially. The duration will further be reduced from time to time.
 29. Review onsite & offsite users as per Segregation of Duties (SoD) like their roles & responsibilities, access level / rights in the proposed technologies and other related onsite / offsite systems etc. on periodic basis and deactivate / modify user access etc. as per requirement with prior approval from the Bank.
 30. Configuration and customization of the tools as per Bank's requirements on ongoing basis.
 31. Feature requests, all critical, showstopper declared by the Bank needs to be implemented within 1 week including thorough functional, performance and security review. There should be no negative functional impact, data loss or performance degradation whatsoever with the introduction of new feature, enhancement, upgrade, bug fixes, customization.
 32. Close every vulnerability in the proposed setup reported in vulnerability assessment (VA) within stipulated time i.e. critical/high risk vulnerability in prescribed timelines, medium/low risk vulnerability within the timelines from the date of reporting of such vulnerability/ observation.
 33. Close every technical and non-technical vulnerability in proposed set-up other than VA such as vulnerabilities observed in internal or external audit / security reviews / SCD implementation, including but not limited to processes, techniques, SOP's etc. within stipulated time i.e. critical/high risk vulnerability in prescribed timelines, medium/low risk vulnerability in prescribed timelines from the date of reporting of such vulnerability / observation.
 34. All the proposed solution must remain compatible with latest encryption and hashing functions.
 35. An automated workflow should be created and maintained for proposed solutions change management initiation, verification, approval, implementation and post-implementation verification.
 36. Proposed solution should be compatible with IPv6 scheme, and there shall be no functional or performance impact on security monitoring due to switch over to IPv6 schema.
 37. Monitoring of alarm conditions that are the result of correlation, pre-defined statistical violation (or baseline alarming) and other activity related to monitoring threat and inappropriate use cases.

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

7.12.1 Continual Improvement

1. Improve the policies configured on an ongoing basis to reduce the occurrence of false positives.
2. Periodic health checks should be carried out by the OEM to ensure the quality of implementation and operations.
3. Bidder shall curtail the closure time for incidents and events and ensure the periodic check-up reviews for the same.
4. Key personnel, including the Project Manager – Operations, Lead – Security Solutions, and Lead – Security Services, Lead L2 and other key personnel proposed by bidder, who are to be deployed during the Facility Management (FM) phase, these individuals should also be actively involved during the UAT and Go-Live phases to ensure continuity and effective execution during FM Phase.
5. Bidder has to develop and maintain Standard Operating Procedures (SOP) for the day-to-day operations of all the solutions to be managed by the Bidder. The SOPs should cover at least vulnerability/ threat management, alert/incident management, MIS reports & dashboards, rules creation & fine tuning, installation/upgradation, signed firmware updates, asset Integration, Business Continuity data & configuration backup, restoration testing, archival, knowledge management, segregation of duties, change management, patch & version management, as per policies of the Bank for all the applications including databases in the

scope. Bidder is expected to create and modify SOPs as per the requirement of the Bank periodically and from time to time, as applicable. All SOPs will be reviewed by the Bank on quarterly basis.

6. Provide post go-live support, which includes but is not limited to system maintenance & support, system performance monitoring, system tuning, root cause analysis, change release management and day to day support (L1, L2, L3), Solution maintenance, SLA compliance etc.
7. Provide support for the platform upgrades, customizations, configurations and resolving bugs/issues.
8. During the support period, the bidder will have to undertake comprehensive support of the platform and all new versions, releases, and updates for all standard product or specified software to be supplied to BANK at no additional cost. The Bidder shall maintain the platform to comply with parameters defined in this RFP.
9. Comprehensive maintenance shall include, among other things, day to day maintenance of the product or specified software a reloading of software, compliance to security requirements, etc. when required or in the event of system crash/malfunctioning, arranging, and configuring facility as per the requirements of BANK, fine tuning, system monitoring, log maintenance, etc. The services and the deliverables should strictly adhere to the SLAs.
10. Support would be comprehensive in nature and must have back-to-back support from the OEMs of the tools and CSP.
11. In the event of system break down or failures at any stage, following shall be specified:
 - a. Diagnostics for identification of product or specified software failures and Root Cause Analysis (RCA)
 - b. Protection of data/ configuration
 - c. Recovery/ restart facility
 - d. Backup of product or specified software / configuration
 - e. The Bidder shall support the Software Solution, tools, and infrastructure provisioned during the entire contract duration as specified in Scope of work in this RFP.
12. The Bidder will be single point of contact and responsible for all, components, software, etc. The bidder must note that the managed services as a part of facilities management should be available for all environments viz., production, training, development, and test.
13. During contract period, the bidder will be responsible for:
 - a. Overall maintenance and working of the solution.
 - b. Bug fixing and delivery of patches/ version changes effected
 - c. Providing tools for creating knowledge repository for the bugs identified, resolution mechanism, version upgrade, future upgrade etc. of Application software, tools, OS, RDBMS, application server software, web server software, interfaces, integrations, customization, reports etc.
 - d. Provision should be available for version control and restoring the old versions if required by BANK
14. Bidder shall provide and implement enhancement/modification/patches/ upgrades/ updates for hardware/ software/ Operating System / Middleware etc. as and when released by Service Provider/ OEM or as per requirements of the Bank. Bidder should bring to notice of the Bank all releases/ version changes.
15. Configuration changes, performance monitoring, troubleshooting, patch installation, running of batch processes, database tuning, replacement / support, technical support, application, and

- data maintenance, taking backup of the database as required, recovery, query generation and management etc. of all software supplied under this RFP document.
16. Immediate bug fixing should be undertaken in the event of software failure causing an interruption of operation as per the response / resolution times defined by BANK. In case of any software /hardware /network failure, the solution should continue to function seamlessly.
 17. All the detected software/hardware errors must be notified and corrected, as per the agreed timelines.
 18. Support BANK in integrating any new applications to the proposed applications
 19. Provide BCP/DR procedures and conduct DR drills in conjunction with BANK policies/procedures
 20. Routing the transactions through backup system in case the primary system fails switching to the DR site in case of system failure
 21. Service records and calls to helpdesk must be maintained and tracked for support, which will be reviewed monthly by BANK
 22. Coordinating and scheduling maintenance activities with BANK and appropriate support functions of BANK/other providers (e.g., network support, facilities support, etc.)
 23. Provide maintenance data, as reasonably requested by BANK, to support replacement / refresh scheduling.
 24. Provide a single-point-of-contact to users for the resolution of problems.
 25. Provide support and assistance, as required, to isolate complex network, operational and software problems related to the proposed solutions
 26. Update, or provide the information required for BANK to update the asset management with BANK
 27. Track and report observed Mean Time Between Failures (MTBF) for Hardware and Software
 28. Release Control shall include the following but not limited to:
 - a. All deliveries (full or patch) shall include a release note containing a full list of the contents of the delivery:
 - b. Versions, file sizes and file modification dates of all components included in the delivery
 - c. All reported faults which are newly fixed in the delivery, identified by fault reference code and including a brief description of the nature of the fix
 - d. All change requests which are completed in the delivery, identified by the appropriate reference code, and including a brief description of the means whereby the change is implemented
 - e. All information required to make any appropriate changes to the tuning and configuration of the production Systems or database such that they continue to meet their specifications
 29. Provide assistance in IT Infrastructure Operations includes but not limited to:
 - a. Major Incident Management
 - b. Determining scope of the problem
 - c. Managing the incident through service restoration
 - d. Validating severity classification of the problem
 - e. Facilitating Service Recovery Team meeting
 - f. Escalating the issue as required
 - g. Conducting Root Cause Analysis
 - h. Preparing restoration plans
 30. Compute Planning includes but not limited to

- a. Configuration Management
 - b. Performance Management
 - c. Capacity Management
31. Provide problem escalation and interact as necessary with third party suppliers.
 32. Provide monitoring and troubleshooting for the entire in-scope solutions & services.
 33. Provide timely notification and escalation to onsite personnel if any hardware and software conditions exist that must be resolved on site to meet the service levels provided in this schedule.
 34. Monitor the status of system processes and events.
 35. Monitor and respond to system alerts and event.
 36. Monitor and maintain system error logs.
 37. Perform application, database, storage replication across the DC & DR as per required Service Levels.
 38. Shifting of IT hardware within the premises, reinstallation and configurations including cabling and asset labelling.
 39. Assist in executing the backup and recovery procedures.

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

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

7.12.2 DR Drill

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

7.12.3 IT Security operations

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

1. The bidder should manage, monitor, maintain and upgrade all IT SECURITY solutions on ongoing basis encompassing all deployed hardware / firmware / middleware / software components by performing timely backups, continuous health monitoring, on-site and offsite support, troubleshooting, critical functional and performance bug fixes, all major product/feature enhancements within the warranty and AMC/ATS charges and as per the SLA defined by the Bank for Contract period.
2. All onsite resources should ensure to deliver the services leveraging IT SECURITY technologies as mentioned in the technology details, architecture and Terms & conditions in the RFP, addendums, corrigendum, clarifications etc. issued by the Bank.
3. The onsite resources must be provided with adequate guidance, assistance & support by competent offsite subject matter experts (SME) of the bidder & OEMs.

4. There should be considerable reduction in MTTD (Mean Time to Detect) and (Mean Time to Remediate) MTTR for security incidents by leveraging technology's own capabilities. All daily routine and standard activities of L1 and L2 to be fully automated.
5. Bidder to ensure efficient utilization and monitoring of Licenses, optimizing capacity utilization, ensuring quality of data and system performance is maintained optimal, there are no security events omission, misfiring rules, heavy rules and reports etc.
6. Participate and contribute to every DR drill, cyber security drill, table-top exercises by the Bank, regulators or any third party.
7. Conduct DR drill of the IT SECURITY on quarterly interval or as and when required by the Bank.
8. Develop custom plug-ins, parsers, connectors, agents, adopters for all the systems in the Bank or related to the Bank periodically or as and when needed without any extra cost to bank.
9. Develop the baseline for the level of logs to be enabled across the different components of IT including infrastructure, databases, business applications and devices etc. The log baselines should be in line with global best practices including NIST, SANS etc. followed by govt., regulatory compliances, Cybersecurity framework and ISO 27001:2013.
10. Perform fortnightly & monthly gap analysis of issues/threat/vulnerabilities in OS, databases, web servers, applications and devices and entire IT infrastructure & recommend and implement remedial actions.
11. Periodically assess the business requirements and configure the required rules, AI/ML based analytics models, self-learning models & processes and generate alerts as per the global best practices and Bank's requirements.
12. The bidder should provide the on-site support for 24/7 around the year (365 days) for the period of warranty, AMC and ATS. L3 support executive should be available during Bank's business hours and whenever required by the Bank during any activity. The support should cover the equipment management, software management, customization, policy installation, maintenance, support, consultation, trouble shooting, forensic analysis etc. As per the bank guidelines, to ensure the effectiveness of business continuity procedure.
13. Creating new reports and customize existing reports, dashboards, rules, queries, user interface in all forms to meet the dynamic requirements of the Bank.
14. Define formats for MIS reporting that include daily, weekly and monthly or any periodical or ad-hoc reports, dashboards as per the Bank's requirements.
15. There should be alert generated and sent to concerned owner(s) for every Potential Security Threat and Incident identified based on the configured rules, and comprehensive AI/ML based modelling on the logs received from the respective Application(s). This mechanism should be based on OWASP foundation and other leading threat modelling Parameters based on the best practices. Unique use cases should be developed and implemented for each business application.
16. Transfer the knowledge to the Bank's IT employees and/or Banks' IT security team about day-to-day operations, system / backend level troubleshooting, dashboarding, creating basic and advanced rules & analytical models, creation and customization of reports & queries etc.
17. End-to-End system level frontend and backend management & maintenance related knowledge need to be transferred to the Bank's staff by the bidder's onsite L1 & L2 resources.
18. There should not be any disruption or degradation in the Bank's network bandwidth utilization and availability due to excessive log transmission or any configurations/customization in the proposed solution.

19. Secure configuration baseline should be benchmarked and updated on a periodic basis with standards including SANS, NIST, CIS etc. followed by Bank's policies, CERT-IN, IDRB, RBI guidelines as updated from time to time.
20. The bidder should use bank provided Ticketing tool identified from time to time for ticketing system, tracking instructions received from application/asset owners like integration, VAPT, incident management etc. Instruction/actionable for the day-to-day operation within the IT SECURITY team should be routed through such tool. Such entries in the ticketing tool should be able to provide activities/jobs completed, pending, pending at which/whose end etc. The performance & turnaround time/efficiency of onsite personnel resource would also be evaluated from the MIS generated from this tool/system.
21. All deliverables including reports, incidents/alerts, their closure, vulnerabilities reported and closed, dashboards, query optimization, indexing, automation based on AI/ML, backup & recovery activities etc. should undergo Quality Assurance process by the onsite resources on an ongoing basis. Project Manager of the bidder and Bidder should define quality metrics, measurement frequency and reporting periodicity in consultation with the Bank.
22. Bidder to ensure security of IT SECURITY setup from cyber-attacks & malwares etc. Any suspicious activity, behaviour of the IT SECURITY setup must be immediately taken into consideration and acted upon at the top priority.
23. For the security of the IT SECURITY setup, bidder should integrate the complete IT SECURITY setup with all the currently & to-be deployed tools and those procured from time to time by the bank.
24. The successful bidder should provide comprehensive AMC & ATS for proposed solutions, including other software, associated modules, hardware and services required to meet the requirements in the RFP.
 - a) The AMC/ATS support for the complete solution should include the following:
 - b) All version upgrades (as per the functionalities and features asked in RFP including the observations raised during VAPT/RBI) during the period of contract at no extra cost.
 - c) Program updates, patches, fixes and critical security alerts as required.
 - d) Documentation updates.
 - e) 24*7*365 support for all the security application related malfunctions and ability to log requests online.
 - f) The Bidder should have back-to-back agreement with the OEMs for ATS and AMC support.

Application management includes but not limited to:

Task	Activities
Services required	1. Installation, configuration, and Un-installation of application 2. Processing Change requests 3. Bug fixing & patch management 4. Vulnerability Assessment and management 5. Data Migration and Uploading 6. Application code migration to new environment 7. Incident and problem management 8. 24*7 Performance Monitoring & Management of application 9. Application Patch management and version control

Task	Activities
	10. Secondary site setup creation and DR management including DR synchronization, DR drill, etc. 11. Perform Primary – secondary site drills (DC-DR Drills) 12. Managing capacity and augmenting in order to meet the SLAs 13. Deploying objects in Application server 14. Troubleshooting Application server product related issues and Patch Management 15. Configure, start, stop, and manage Server services for all environment and nodes as required. 16. Configure and manage HTTP/HTTPS 17. Configure and use monitoring tools provided for Application Server 18. Backup & restoration management of application server 19. Performance management 20. Vendor management (Logging a call with product Vendor) 21. Version migration, testing and implementation 22. File Level Backup of compute 23. Portal/content management. 24. User management 25. Support to known errors and problems 26. Monitor web / Application server availability 27. Monitor alert notifications, checking for impending problems, triggering appropriate actions. 28. Bidder is required to factor in a solution to automate the batch jobs to meet the requirements of the RFP.

25. Incident, Problem and performance Management Services

- a. Bidder needs to provide below mentioned services but should not limit itself to this list:
 - i. Account administration and access management within the proposed security solutions.
 - ii. Performance monitoring, incident management, and problem management for the proposed security solutions.
 - iii. Monthly and fortnightly incident, event, alert, and service analysis.
 - iv. User rights, role, and privilege administration within the proposed security solutions.
 - v. Monitoring solution availability, service health, integrations, log collection status, processing performance, storage utilization, database growth, and application performance.
 - vi. Preparation of preventive maintenance schedules, health check reports, capacity utilization reports, and root cause analysis reports for the proposed solutions.
 - vii. Implementation and validation of application patches, hotfixes, signatures, threat intelligence updates, content updates, and security updates released by the respective OEMs.
 - viii. Security hardening and secure configuration management of the proposed security solutions.
 - ix. Troubleshooting alerts, incidents, errors, and performance issues related to the proposed security solutions.

- x. Incident resolution, tracking, escalation, and closure.
- xi. Participation in DC-DR failover, restoration, and business continuity testing activities related to the proposed security solutions.
- xii. Coordination and escalation with OEMs, infrastructure teams, cloud service providers, and other vendors as required.
- xiii. Review and audit of privileged accounts, administrative activities, logs, and audit trails within the proposed security solutions.
- xiv. Validation of backup, restoration, archival, and recovery activities related to configurations, policies, rules, use cases, dashboards, reports, and solution databases.
- xv. Log monitoring, analysis, correlation, retention, archival, and lifecycle management.
- xvi. Restoration and recovery drills for the proposed security solutions.
- xvii. Definition of backup requirements, validation of backup schedules, and coordination for resolution of backup failures with the respective infrastructure teams.
- xviii. Performance tuning, optimization, and capacity planning of the proposed security solutions.

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

7.12.4 OEM Services & Deployment (Architecture Assessment):

Assessment & performance review

1. Review of respective solutions configurations (Custom parsers, playbooks, controls, rules and process etc.) of the OEM solution
2. System Optimization review and suggestion including remedial actions.
3. Review the bidder's implementation of suggestions of remedial actions.
4. List of Solution for which Assessment is to be conducted are:
 - a) SSL Orchestrator with Packet Broker
 - b) Web Application Firewall
 - c) Data loss prevention
 - d) Zero-Day Attack Protection at Endpoint and Network
 - e) Database Activity Monitoring
 - f) Identity and Access Management
 - g) Privileged Identity Management
5. Incident Handling and OEM Involvement:
 - a) For any concerns, incidents, issues or identified threats/vulnerabilities etc.—especially those classified as critical—the bidder is required to engage with the respective OEMs at regular intervals to ensure timely and effective resolution.
 - b) Furthermore, any resolution proposed or implemented by the bidder for a critical-level incident must be reviewed and formally certified by the respective solution's OEM ensuring that the resolution aligns with OEM best practices, maintains system integrity, and does not introduce new risks or vulnerabilities.
 - c) Regular collaboration with OEMs should also include proactive reviews, patch advisories, configuration validation, and support for root cause analysis, where applicable.

7.12.5 System recovery

1. In case of disaster, it is the responsibility of the Respective solution OEM along with the bidder to ensure that services remain unaffected and same is up and running from secondary site (DR)
2. It is bidder's responsibility to maintain DC – DR patches, updates & upgrades on continuous basis. Bidder to ensure that scheduled / unscheduled DR drills is conducted on regular basis (Quarterly basis or as defined by BANK). As part of these exercises, bidder to submit compliance / completion of activity reports at the end of the activity.
3. Bidder is responsible for performing DR drills between the proposed primary (DC) & secondary site (DR). Also, bidder to participate and assist BANK in their DR drill (planned & unplanned) and ensure the availability of solution during BANK's drills. During the DR Drills, bidder to ensure that full manpower deployment is made available during the drill.
4. Processes shall be in place to allow for recovery to a disaster recovery hardware platform, and the bidder shall provide Estimates of recovery time.
5. Proposed method of recovering the logical state of the production service, Likely extent of data loss in the event of such recovery being required
6. The Bidder shall maintain following documentation and same shall be shared during the start of the project and every MONTH highlighting the updates made in the document with respect to the previous version.
 - a) Disaster Recovery Plan- identifying the operations involved in disaster recovery and the dependencies between these operations.
 - b) Disaster Recovery Procedures- providing step-by-step instructions for the operations identified in the Disaster Recovery Plan
 - c) Disaster Recovery Test Plan- identifying the steps and resources required to carry out a Disaster Recovery test to validate the Disaster Recovery Plan and Procedures
7. The Bidder shall ensure that each batch job (if any) can, following a failure, be restarted from the point of failure once the cause of the failure has been removed

7.13 IT Infrastructure

1. The bidder shall be responsible for the supply, installation, configuration, integration, testing, commissioning, documentation, warranty, and comprehensive maintenance of the proposed IT infrastructure throughout the contract period. This includes all hardware, software, licenses, operating systems, firmware, accessories, cables, and associated components required for successful deployment. The bidder shall also provide preventive and corrective maintenance, firmware and software updates, security patches, OEM support, replacement of defective components, and technical assistance to ensure continuous availability and performance of the deployed infrastructure in accordance with the prescribed SLAs.
2. The list of major activities in the scope, inter alia, is placed below:
 - i Supply of requisite hardware and software
 - ii Stack Deployment and Commissioning including virtualization if required
 - iii System Integration, Testing, Acceptance and Sign Off.
 - iv Compliance to bank's Security configuration document for the proposed infrastructure
 - v Technical documentation
 - vi DC, DR & NDR Implementation
3. The bidder shall deliver a fully functional, secure, highly available, and scalable infrastructure conforming to the Bank's technical, operational, security, and regulatory requirements.
4. Supply of IT Infrastructure
 - i The bidder shall supply all hardware, software, operating systems, hypervisors, firmware, appliances, licences, accessories, power cords, optics, transceivers, cables, mounting kits, documentation, and other components required for complete deployment of the proposed solution.
 - ii All equipment should be new, unused, genuine, and sourced directly from the OEM.
 - iii Necessary firmware, BIOS, and software versions recommended by the OEM shall be installed.
 - iv Ensure servers include sufficient CPU cores, RAM, and network interface cards (NICs) to handle expected transaction volumes, data processing needs, parallel operation of Backup & Restoration (with Ransomware Protection) and Replication.
 - v Ensure proposed storage Confirm compatibility with servers, database, Backup & Restoration (with Ransomware Protection) Solution and existing infrastructure & software requirements, ensuring expansion options for future scalability.
 - vi Supply necessary components such as SFPs, power units specific to the proposed hardware to support hardware.
 - vii Ensure cables and connectors meet performance standards to prevent signal degradation or data loss
 - viii Right size and factor adequate licenses of OS, Db, Application server software, web server software and any other tool/software to meet the requirement of the RFP.
 - ix Bidder/OEM is required to only propose Enterprise/OEM Supported based licenses
5. Installation and Deployment
 - i Any support (like OS Installation/Re-Installation, patching, configurations etc.) required by OEM during installation or post installation must be provided by the bidder/OEM as part of the overall scope of the RFP.
 - ii The bidder/OEM is responsible for supplying, designing, sizing and configuring the Backup Software and Hardware (with Ransomware Protection). The backup

solution configuration should comply with bank's policy for secure data backup, with flexibility for updates as policies evolve. Sizing should align with the overall storage requirements.

iii The Bidder/OEM shall perform complete installation and deployment of the proposed infrastructure at the Bank's Data Centre (DC), Disaster Recovery (DR) site, Near DR site, or any other designated locations.

- Installation activities shall include, but not limited to:
 - Rack mounting and physical installation.
 - Power connectivity and cable management.
 - Network connectivity.
 - Hardware assembly and configuration.
 - Firmware and software installation.
 - Device labelling and asset tagging.
 - Physical and logical connectivity validation.
- Configuration and Implementation Services, but not limited to
 - **Compute Infrastructure**
 - Server installation and configuration.
 - BIOS and firmware configuration.
 - Operating system installation.
 - RAID configuration.
 - Network interface configuration.
 - Server hardening.
 - Cluster configuration.
 - **Storage Infrastructure**
 - Storage installation and configuration.
 - RAID and storage pool configuration.
 - Logical volume creation.
 - Storage provisioning.
 - SAN zoning and host mapping.
 - Multipathing configuration.
 - Storage performance optimization.
 - **Network Infrastructure**
 - Switch configuration.
 - VLAN configuration.
 - Routing configuration.
 - High Availability configuration.
 - Port configuration.
 - Access control configuration.
 - **Network Infrastructure**
 - Switch configuration.
 - VLAN configuration.
 - Routing configuration.
 - High Availability configuration.
 - Port configuration.
 - Access control configuration.

iv Integration with Existing IT Environment, but not limited to

The Bidder shall integrate the proposed infrastructure with the Bank's existing IT ecosystem.

- The integration scope shall include:
 - Existing network infrastructure.
 - Existing storage environment.
 - Security infrastructure.
 - Monitoring and management platforms.
 - Identity and access management systems.
 - Enterprise applications, wherever applicable.

The Bidder shall ensure seamless interoperability and minimum disruption to existing business operations.

6. Warranty, ATS, AMC and Support services, but not limited to
 - i The bidder should provide services related to warranty, maintenance, and support of all the software, application, and hardware inventories for the entire contract period at all locations of Bank (DC / DR/ NDR).
 - ii The bidder should provide maintenance of Hardware but not limited to preventive Hardware support, repair and / or replacement activity after a problem has occurred, Firmware upgrade, Warranty service & support of network, security, server, storage, backup & DB.
 - iii If the Hardware/Software supplied/taken handover by the bidder is to be replaced permanently, then the bidder shall inform the Bank well in advance prior to replace the respective equipment failing which the bidder will be liable for penalty as per this scope document furnished elsewhere.
 - iv The bidder should provide a Single Point of Contact to Bank for the resolution of Hardware related problems or to request an equipment upgrade or consultation.
 - v Bidder should coordinate and schedule hardware maintenance activities in co-ordination and approval with Bank
 - vi Defect Liability - In case any of the supplies and equipment delivered under the Contract are found to be defective as to material and workmanship and/or not in accordance with the requirement, and/or do not achieve the guaranteed performance as per the requirement, within the warranty and AMC period (if contracted) of the contract, the Managed Service Provider shall forthwith replace/make good such defective supplies at no extra cost to the Bank without prejudice to other remedies as may be available to the Bank as per scope terms.
 - vii Bidder should take prior permission from the Bank for any planned downtime for maintenance and Bidder should follow the bank change management process.
 - viii End-to-End Incident, Problem & Service Restoration Management
 - Manage incidents, restore services within SLA, perform RCA, prepare restoration plans, maintain problem records, and drive resolution through structured escalation and change management.
 - ix 24x7 Infrastructure Operations, Monitoring & Performance Management
 - Continuously monitor and manage servers, databases, storage, networks, hardware, system software, alerts, logs, capacity, performance, availability, and automation to ensure optimal uptime.
 - Provide end-to-end operations, monitoring, and management of compute, servers, storage, databases, virtualization, networks, and security infrastructure across DC, DR, and NDR.

- Perform operating system administration, server configuration, user/account management, OS hardening, antivirus management, patching, system tuning, and server lifecycle management.
 - Continuously monitor infrastructure health, resource utilization, application availability, logs, alerts, capacity, and performance, while implementing optimization measures.
 - Configure and administer SAN/NAS infrastructure, storage arrays, FC switches, LUNs, snapshots, replication, storage virtualization, migrations, and capacity planning.
 - Install, configure, monitor, secure, tune, patch, upgrade, recover, replicate, and optimize databases while managing capacity, archival, and high availability.
- x Configuration, Change & Release Management
- Implement and maintain configuration management, operating system standards, patches, software upgrades, hardware refreshes, release management, rollback plans, and all approved changes in coordination with the Bank.
 - Implement, maintain, and control infrastructure configurations, software releases, patches, firmware updates, and approved changes with impact assessment and rollback planning.
- xi Backup, Disaster Recovery & Business Continuity
- Execute backup, restoration, replication (DC/DR/NDR), disaster recovery drills, failover testing, high availability, clustering, and recovery planning to ensure business continuity and data protection.
- xii Information Security, Compliance & Vulnerability Management
- Enforce security hardening, access control, antivirus, patch management, vulnerability remediation, VA/PT findings, security logging, compliance with Bank policies, and regulatory/security mandates.
- xiii Identity, Access & Privileged Account Administration
- Manage user IDs, privileged access, account lifecycle, periodic access reviews, security permissions, authentication controls, and compliance with approved change and security processes.
- xiv Asset, Documentation & Audit Management
- Maintain accurate asset inventory, infrastructure documentation, SOPs, configuration diagrams, audit trails, operational logs, installation records, and support closure of audit observations.
- xv Vendor, OEM & Stakeholder Coordination
- Coordinate with OEMs, third-party vendors, SOC, Bank teams, and support partners for issue resolution, upgrades, preventive maintenance, licensing, escalations, and communication.
- xvi Capacity Planning, Optimisation & Operational Automation
- Perform capacity planning, resource forecasting, performance tuning, workload optimisation, batch scheduling, automation, preventive maintenance, and continuous service improvement.
- xvii Governance, SLA Compliance & Service Delivery Management
- Ensure adherence to SLAs, maintain escalation matrices, deploy adequate onsite resources, provide governance reporting, manage service delivery,

obtain Bank approvals for changes, and ensure overall operational excellence and contractual compliance.

- Maintain operational documentation, reports, audit evidence, log retention, compliance records, inventory, and provide complete support for internal, external, and regulatory audits.
7. The Bidder shall ensure adherence to industry best practices and the Bank's infrastructure standards during deployment.
 8. The Bidder shall confirm/ certify that the hardware sizing offered by them for Solution should be adequate to fulfil bank's requirement, SLAs and terms of the RFP.
 9. Bidder's need to provide the Sizing on the bank's provided configuration mentioned in Appendix 2: Masked Bill of Material and Appendix 3: IT Infrastructure Virtual to Physical mapping. Bidders need to provide sizing, which is required for DC, DR and Non-Production environment.
 10. Bank would provide the following IT Hardware components, sizing of which shall be provided by bidder in their technical proposal:

1	TOR Switch
2	Racks

11. IT Infrastructure managed services
 - i Infrastructure Operations and Management.
 - ii Infrastructure Monitoring and Event Management.
 - iii Incident, Problem, Change, and Request Management.
 - iv Compute, Storage, Backup, Network, Virtualization, Database, Cloud, and Security Infrastructure Management.
 - v Patch Management and Vulnerability Remediation Support.
 - vi Capacity Planning and Performance Optimization.
 - vii OEM Coordination and Support Management.
 - viii Preventive and Corrective Maintenance.
 - ix IT Service Management (ITSM) Operations.
 - x Documentation and Reporting.
 - xi Knowledge Transfer and Transition Management.

The Bidder shall provide all necessary manpower, tools, processes, and expertise required for successful delivery of managed services.

12. The bidder should also get the confirmation from the Solution's OEM regarding hardware sizing proposed and submit the confirmation from each of the OEM on the sizing of their respective product.
- The bidder is required to provision, provide and factor in associated cost for all requisite components (except for the component mentioned in the above table) for successful deployment, implementation and management of the solutions & services sought in the RFP.

The following considerations need to be taken for sizing:

- a. The bidder shall be solely responsible for sizing all infrastructure components required for the proposed solution. The sizing shall be based on the requirements specified in the RFP and shall adequately cater to performance, availability, security, retention, disaster recovery, scalability, and projected growth during the entire contract period.
- b. The bidder shall ensure that the proposed sizing is sufficient to meet all functional, technical, performance, and Service Level Agreement (SLA) requirements specified in the RFP.

- c. The Bidder shall ensure Hardware lifecycle management covering installation, preventive maintenance, refresh, and support.
- d. Performance and capacity management through proactive monitoring, trend analysis, and resource planning.
- e. Job scheduling, automation, and monitoring of batch processes and critical business workloads.
- f. Continuous vulnerability assessment, remediation, and compliance with security advisories.
- g. Continuous service improvement through automation, process optimization, knowledge management, and adherence to industry best practices.
- h. The Bidder shall be solely responsible for the accuracy and adequacy of sizing all IT infrastructure components required to meet the RFP requirements and prescribed SLAs throughout the Contract Period. Any deficiency arising from incorrect sizing, underestimation, or inadequate capacity planning shall remain the Bidder's responsibility.
- i. The Bank shall not be responsible for any assumptions, estimates, calculations, sizing methodologies, or judgments made by the bidder while arriving at the proposed architecture, sizing, volumetrics, or commercial bid. The bidder shall be deemed to have independently assessed all requirements of the RFP and shall remain fully responsible for the adequacy and accuracy of the proposed sizing. The Bank shall evaluate the bidder's performance against the requirements, specifications, service levels, and outcomes defined in the RFP and the resultant contract.
- j. Upon recording an SLA breach or identifying an infrastructure shortfall attributable to inadequate/incorrect sizing, the Bank shall seek an augmented sizing plan from the Bidder. The Bidder, in consultation with the respective OEM(s), shall submit the revised sizing and additional infrastructure requirements within the timelines specified by the Bank.
The Bank may adopt following option for procurement/addressing the shortfall and can exercise any of the below option at its sole discretion:
 - i. Option 1: Bank may procure the additional infrastructure required to restore SLA compliance through an appropriate procurement mechanism. The cost incurred by the Bank for such augmentation, along with applicable SLA penalties, shall be recoverable from the Bidder and may be deducted from any payments due under the Contract.
 - ii. Option 2: Bank may allow bidder to provide and implement the additional infrastructure, licenses, software, or components necessary to ensure compliance with the RFP requirements and applicable SLAs. Such augmentation shall be carried out by the Bidder at no additional cost to the Bank within the timelines mutually agreed with the Bank in writing.

7.14 Other In-Scope services

7.14.1 Other Scope Activity

1. The Respective solution OEM along with the bidder is expected to ensure that all functionalities as mentioned in Appendix 1A: Functional Specification are made available to PSB.
2. The Respective solution OEM along with the bidder is expected to ensure that for the purpose of this RFP, statutory and regulatory changes shall mean any change prescribed by the statutory and regulatory bodies governing/ affecting the banking industry in India viz. Reserve Bank of India, Ministry of Finance, CCIL, NPCI, IBA, SEBI, or any such bodies constituted by the RBI mandating change/s to an existing functionality of the Solution shall be provided to the Bank at no additional cost for the entire contract period. However, any Statutory and Regulatory changes post

complete Go-Live of the respective applications (which are not a part of the existing functionalities) will be on CR basis based on the rates provided in the Bill of Material.

3. The Respective Solution OEM along with the bidder is expected to carry out a requirement study for the functionalities and services required by PSB, to gain understanding of the business requirements.
4. Respective solution OEM along with the bidder must note that it shall not be permitted to change the proposed OEM Solution after submission of bid. Bidder must also note that it shall not be permitted to quote any options of solution/OEM. Failure to adhere to this clause may attract disqualification of the bid / contract as well as invoke related damage clauses as specified in Terms and Conditions.
5. The Respective Solution OEM along with the bidder is expected to customize the screens, design and layout of the solution depending on the requirements of the bank, at no additional cost to the bank as per the specific UI/UX design finalized during the SRS
6. The Respective solution OEM along with the bidder is expected to customize the solution based on the requirements of bank.
7. The Respective solution OEM along with the bidder is expected to support the bank in the installation, implementation, rollout and maintenance of all the proposed applications.
8. The Respective solution OEM along with the bidder is responsible to impart requisite training to the bank officials as per the ask of the RFP
9. The Respective solution OEM along with the bidder has to ensure the seamless switching of all the services to Disaster Recovery (DR) site during DR drill as and when decided by Bank or in case of non- availability of primary/ DC site.
10. The Respective Solution OEM along with the bidder needs to mention any other security feature supported by the system with details and architecture of the security components.
11. The Respective solution OEM along with the bidder is required to make changes in the Solution including software, procedure and operations as required by regulators from time to time to comply with any new rules of Indian Law, RBI, IBA, TRAI, Govt. of India, NPCI guidelines and other Regulator body for all the Proposed Solutions.
12. The Bidder should ensure continual security of the software/solution. Any development activity for incorporating security measures should be a part of the ATS.
13. The hosting Space and Power arrangement shall be provided by the Bank at DC and DRC. However, the bidder is required to factor in the requisite racks in order to successfully operationalize the proposed hardware.
14. It is the responsibility of the Respective Solution OEM along with the bidder to resolve any deficiency identified in the performance of Proposed Solutions, as observed during the acceptance test. This includes replacement of some or all equipment at no additional cost to the Bank, to ensure that the solution meets the requirements of the Bank as envisaged in the RFP.

7.14.2 Transition Management

1. The Bank shall provide the Selected Bidder complete details of the existing security infrastructure, deployed solutions, architecture diagrams, inventory, integrations, licenses, OEM support contracts, operational procedures, and incumbent vendor support arrangements as available with the bank during the project initiation period.
2. The bidder shall take over and maintain operations of the bank's existing solutions starting 01.05.2027 and continue doing so until the new proposed solution goes live, in accordance with the RFP.

3. The Bank shall enable adequate cooperation and knowledge transfer support from the incumbent service provider(s). However, it is the responsibility of the bidder to liaison with the existing vendors and the OEMs.

7.14.3 Security Management

1. Authentication and authorization mechanism for all users and systems should ensure enforcing bank's security policies.
2. End to end security mechanism to ensure security of logs, data, information, alerts, users, configurations etc. at rest / storage / database, during processing and in transit.
3. User id and login should determine level of access to data e.g. read/view data, print data, write/modify data, delete data etc.
4. The solution should support the following security features:
 - a. Username and password for accessing the applications and database
 - b. Access credentials should not be stored on the endpoints
 - c. Auto blocking/locking of applications access upon reaching maximum number of tries.
The maximum number of incorrect errors should be defined by the Bank
5. Termination of session and log off after lapses of configurable time period.
6. The solution should support the following transaction level security:
 - a. End-to-End encryption of data transmission (symmetric or asymmetric)
 - b. The solution should support multiple authentication-based bank's preferences
7. The solution should support the following platform security & reliability:
 - a. Data stored is encrypted in the platform database
 - b. Audit trails and logging features must be available in Web Server, application server and database server
 - c. Ability to assign specific rights to platform administrators for secure and restricted access
 - d. Solution should have the ability to support external certifying authority
 - e. Solution should have secure interfaces to various hosts systems according to prevailing security standards
 - f. Application access credentials should not be stored locally.
 - g. Solution should support standard algorithms like AES
 - h. Solution should have a minimum encryption strength of 256 bit for end-to-end transaction (Standard encryption algorithms like 3DES, AES, PKI scheme, with minimum encryption strength of 256 bit)
 - i. The predefined pages of the web portal should handle web application security threats like Cross-site scripting, SQL injection flaws, Malicious file execution, Information leakage, Improper error handling, Broken authentication and session management, Insecure Cryptographic storage, Failure to restrict URL access.
 - j. Platform should have a clear separation of security responsibilities and should be designed for externalized security implementing JAAS (Java Authentication and Authorization Services) allows for pluggable providers
 - k. OWASP Top 10 Compliant
 - l. Password must be hashed by SHA256 at least and include Salt or using salt supported cryptography
 - m. All the sensitive data (e.g. passwords), including their backups, stored in an encoded or encrypted form in order not to be readable in case of exploitation or other application corruption
 - n. Sensitive Data Exposure:

- i. Sensitive data should be masked when output.
 - ii. Sensitive data should not be stored in source code, config files and logs.
 - iii. Passwords are hashed using Salt.
- o. Configurable approval rules set up for Bank administrator to perform the actions
- p. Regulatory & Statutory
 - i. The solution should comply with the security principles and practices as stipulated by Statuary and regulatory authorities in India
- q. Application
 - i. OS Security check up. Application should have capability to detect if the application is running on a jail-broken / rooted / malware infected device.
 - ii. Application must prevent hackers from accessing the application in a case where the device is rooted or jail broken.
 - iii. Blacklisting/Blocking of older versions of the Application on the back end, if there is a security breach.
- r. Transaction Logs
 - i. Should maintain detailed transaction logs to enable processing audit trails to be reconstructed in the event of any disputes or errors
 - ii. The storage and retention period of logs should be parameterized
 - iii. Security safeguards should also be implemented to protect the information from unauthorized modification or destruction
 - iv. System should facilitate maintaining logs.
 - v. Provision to generate detailed reports, logs, audit trails

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

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

8 CONTRACT PERIOD

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

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

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

The bank may, at its sole discretion, extend the contract for an additional period of two years, in one-year increments tranches. The Bank may extend the support services for an additional period of up to two (2) years beyond the original contract period. The pricing applicable during the extension period shall be mutually agreed and shall not exceed 110-120% of last year's AMC/ATS/Facility management rates quoted by the Selected Bidder.

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

End of Sales / End of support: The bidder must ensure that any equipment (hardware/software) supplied as part of this RFP should not have either reached or announced end of sales as on the date of such supply or end of support for at least duration of the contract (including the period of 2-year extension).

In the event if any equipment supplied by the bidder reaches the end of support, within the contract period, the bidder has to replace the equipment/component at no additional cost to the Bank.

During the extension period, if any product goes end of support bidder is required to provide the extended OEM support for proposed product or provide the bank with the alternative product of similar/higher configuration from OEM (with requisite support) at no additional cost to the bank.

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

9 PROJECT TIMELINES

Overall Implementation period shall be 5 Months (Start Date is T0) for all solution & services

The bidder shall submit a comprehensive Project Plan, within 7 days of T0 covering each proposed product/solution & Services, detailing all project phases, milestones, tasks, sub-tasks, activities, timelines, dependencies.

The bidder shall submit the detailed Project Plan within seven (7) days from T0 for the Bank's review and approval.

Any Liquidated Damages (LD) for delays in project execution shall be calculated based on the bank's approved Project Plan.

In the event the bidder fails to submit the Project Plan within seven (7) days from T0, the Bank reserves the right to levy applicable Liquidated Damages for each day of such delay. If the delay in submission

of project plan exceeds seven (7) days, the Bank may prepare and issue the Project Plan, which shall be final and binding on the bidder.

The bidder shall execute the project in accordance with the Bank-issued Project Plan, maintaining the overall implementation period of five (5) months from T0.

All applicable Service Level Agreements (SLAs), milestones, Liquidated Damages (LDs), and other contractual obligations shall thereafter be governed by the Bank-issued Project Plan, which shall be deemed to have been accepted by the bidder without any further objection or reservation.

All the requirement marked by bidder as “S” and “C” has to be delivered before UAT

T0- Date of acceptance of PO

Architecture Assessment:

Review is to be conducted annually, from year 2 onwards (Post go-live of respective solutions) on a yearly basis- within 15 days of bank notifying the bidder to initiate the assessment.

10 EVALUATION CRITERIA

10.1 Preliminary Scrutiny

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

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

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

During evaluation of the Tenders, the Bank, at its discretion, may ask the Bidder for clarification in respect of its tender. The request for clarification and the response shall be in writing, and no change in the substance of the tender shall be sought, offered, or permitted. The Bank reserves the right to accept or reject any tender in whole or in part without assigning any reason thereof. The decision of the Bank

shall be final and binding on all the bidders to this document and the bank will not entertain any correspondence in this regard.

Bidders are therefore advised to ensure that all required documents and supporting evidence are submitted along with the bid. The Bank shall evaluate the bid based on the documents submitted and the Bank's decision regarding the adequacy, relevance, interpretation, compliance, and evaluation of the submitted documents and information shall be final, conclusive, and binding on all bidders.

10.2 Eligibility Evaluation Criteria

Eligibility criteria to be met mandatorily by the bidders:

#	Eligibility Criteria/Clause	Supporting Documents
1	Proof of Earnest Money Deposit	To be submitted along with the bid.
2	The Bidder should be operating in India as a registered company under Companies Act, 2013/1956 or LLP (Limited Liability Partnership) Act 2008 or Partnership firms registered under the Indian Partnership Act, 1932 with registered offices in India, and should be in existence in India for at least the last 5 (five) years as on date of opening of the bid	• Copy of Certificate of Incorporation or Partnership Deed • Copy of Registration Certificate/GST Registration certificate Copies of all documents listed above should be attested by authorized signatory and must be submitted along with the response.
3	The bidder should have valid PAN and GST Registration in India	Copy of Valid PAN Card and GST Registration Certificates issued by competent authority in India
4	The bidder should have a minimum average annual turnover of INR 1000 crore in India during the last 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth.	• CA Certificate* mentioning the turnover and net worth for each financial year and • Financial statements Audited (Balance sheet & Profit & Loss statement). The *CA certificate provided in this regard should be without any riders or qualification.
5	The bidder should be an authorized representative/ partner/ reseller of each of the proposed OEMs in India. MAF should be submitted from the following solution OEMs: 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. SSL Orchestrator along with packet broker 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network 6. Zero Trust Network Access (ZTNA) 7. Data Loss Prevention (DLP)	MAF from the respective OEMs of the solution & services containing- 1. Name and address of the OEM and the name and address of the authorised bidder/entity. 2. Confirmation that the OEM shall honour and extend warranty and support for the products and services supplied by the authorised bidder/entity. 3. Confirmation that the bidder/entity is duly authorised by the OEM for supply, installation, implementation,

#	Eligibility Criteria/Clause	Supporting Documents
	8. Information/Digital Right Management 9. Database Activity Monitoring 10. Mobile SDK 11. Host IPS including Application Change Control (HIPS) 12. Web Application Firewall (WAF) 13. Centralized key management solution 14. Certificate Lifecycle management 15. Identity & Access Management Solution 16. Multi Factor Authentication 17. Privilege Identity/Access Management 18. DNS Security Services (Internet-Facing DNS Security Services) 19. Cloud Access Security broker (CASB) 20. AI Security 21. SBOM/CBOM/AIBOM/QBOM	technical support, maintenance and related services for the proposed solution(s). The MAF shall be submitted on the official letterhead of the respective OEM and must be signed by an authorised signatory having the authority to bind the OEM.”
6	Bidder must have at least enrolled manpower (on bidder’s payroll) of 150 experienced employees skilled in areas of Cyber/IT security.	Self-certification from the bidder
7	Bidder should have supplied, installed and maintained (or under maintenance) at least 10 of the below solutions in any one PSU/PSE/ BFSI/Government Organizations/ Regulatory & Statutory body in India: 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. SSL Interception/SSL offloader 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network/Anti-APT 6. Zero Trust Network Access (ZTNA)/Remote Access VPN 7. Data Loss Prevention (DLP) 8. Information/Digital Right Management 9. Database Activity Monitoring	Copy of Purchase Order/Work Order/ Contract AND In addition to the above, bidder to provide the following: a) Client credential/reference letter specifying the product deployed and the current status/stage of the project; OR b) Email confirmation from the client specifying the product deployed and the current status/stage of the project; OR c) Client-signed implementation signoff/ report confirming successful implementation of the solution;

#	Eligibility Criteria/Clause	Supporting Documents
	10. Mobile SDK 11. Host IPS including Application Change Control (HIPS) 12. Web Application Firewall (WAF) (Mandatory Requirement) 13. Centralized key management solution 14. Certificate Lifecycle management 15. Identity & Access Management Solution 16. Multi Factor Authentication/2FA 17. Privilege Identity/Access Management 18. DNS Security Services (Internet-Facing DNS Security Services) Note: - a. Experience of solutions can be shown in single /multiple Clients/ work orders meeting the above criteria b. A bidder's experience in supplying and installing a solution will be considered regardless of when the installation was completed. Even if the installation was completed more than five years ago, it will still qualify, provided the bidder is currently maintaining that solution or has carried out its maintenance at any time during the five-year period preceding the RFP publication date.	Note: The submitted documentary evidence must clearly identify the customer, the product/solution deployed, and the implementation and/or maintenance status relevant to the criterion for each of the products.
8	Bidder must have back-to-back support relation with all the proposed OEMs of solutions & services.	Self-Declaration from the bidder's authorized signatory stating the following: “We M/s _____ confirm that we shall backline with the respective solutions & services OEMs proposed through this RFP within 1 month of issuance of the Purchase order. We shall submit the relevant copy of the backlining agreement/ excerpt of the agreement/OEM confirmation for the duration of the contract” to substantiate the said clause.

#	Eligibility Criteria/Clause	Supporting Documents
9	If the bidder or its subsidiary or its associate or sister company or its holding company has already had an association with Punjab & Sind Bank in the past 5 years or at present as a service provider on any project, then the bidder is required to submit the satisfactory certificate from the bank issued/dated post the issuance of the RFP. Additionally, the Bidder should not have any Service Level Agreement/Contract pending to be signed with the Bank pending for more than 6 months from the date of issue of purchase order	Self-Certification from the bidder along with the satisfactory certificate from PSB (In case of association)
10	The Bidder to provide information that none of its subsidiaries or sister company or associate or holding company or companies having common director/s or companies in the same group of promoters/management or partnership firms/LLPs having common partners is not owned by any Director or Employee of the Bank.	Self-Certification from the bidder
11	The bidder shall submit a self-declaration confirming that, during the last three (3) years preceding the date of publication of this RFP, no contract, Purchase Order, or award issued by Punjab & Sind Bank (PSB) to the bidder has been cancelled, terminated, rescinded, or revoked due to non-performance, breach of obligations, or failure to comply with post-award requirements.	Self-Certification from the bidder
12	The Bidder should not have been blacklisted/ debarred by the Regulator / statutory body/ Government / Government agency / Banks / Financial Institutions in India during last 3 years and as on the date of bid submission.	Self-Certification from the bidder as per Annexure 11
13	The bidder should not be involved in any litigation which threatens the solvency of company.	Self-Certification from the bidder as per Annexure 10
14	Labor Law Compliance	Self-Certification from the bidder
15	Integrity Pact	Document on 100 Rs Stamp paper, duly signed and stamped by the authorized signatory.
16	Non-Disclosure Agreement	Document on 100 Rs Stamp paper, duly signed and stamped by the authorized signatory.

#	Eligibility Criteria/Clause	Supporting Documents
17	To avoid conflict of interest the successful bidder or its subsidiary or its associate or sister company or its holding company should not be the nextGEN SOC /SOC vendor of the bank under the existing	Self-declaration signed by Authorized Signatory of the bidder.
OEM Evaluation Criteria		
18	The proposed OEM solution/product should have been successfully implemented in least two Scheduled bank (including financial regulators). The reference implementation need not be of the same model, version, or product family as the proposed solution. List of Product which is required to comply with the above clause 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. SSL Orchestrator along with packet broker 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network 6. Zero Trust Network Access (ZTNA) 7. Data Loss Prevention (DLP) 8. Information/Digital Right Management 9. Mobile SDK 10. Host IPS including Application Change Control (HIPS) 11. Web Application Firewall (WAF) 12. Centralized key management solution 13. Certificate Lifecycle management 14. Database Access Management (DAM) 15. Identity & Access Management Solution 16. Multi Factor Authentication 17. DNS Security Services (Internet-Facing DNS Security Services)	Copy of Purchase Order/Work Order/ Contract In addition to the above, bidder to provide the following: “A client credential letter or email from the customer confirming the product used and the current stage of the project OR A client-signed implementation report or official sign-off confirming the work OR Self-Declaration from OEM confirming the product & stage of the project and reference to the PO”

#	Eligibility Criteria/Clause	Supporting Documents
	Note: Experience should be during the five-year period preceding the RFP publication date. Even if the installation was completed more than five years ago, it will still qualify, provided the product is currently under maintenance or has been maintained at any time during the five-year period preceding the RFP publication date	
19	The proposed OEM solution/product for Privilege Identity/Access Management should have been successfully implemented in at least 2 BFSI in India, out of which at least one (1) BFSI Client should have a deployment covering more than 1,500 privileged users Note: Experience should be during the five-year period preceding the RFP publication date. Even if the installation was completed more than five years ago, it will still qualify, provided the product is currently under maintenance or has been maintained at any time during the five-year period preceding the RFP publication date	Copy of Purchase Order/Work Order/ Contract In addition to the above, bidder to provide the following: “A client credential letter or email from the customer confirming the product used and the current stage of the project OR A client-signed implemented report or official sign-off confirming the work OR Self-Declaration from OEM confirming the product & stage of the project and reference to the PO”
20	The proposed OEM solution/product should have been successfully implemented in at least 2 verifiable clients in India. The reference implementation need not be of the same model, version, or product family as the proposed solution. List of Product which is required to comply with the above clause 1. AI Security 2. SBOM/CBOM/AIBOM/QBOM	Copy of Purchase Order/Work Order/ Contract In addition to the above, bidder to provide the following: “A client credential letter or email from the customer confirming the product used and the current stage of the project OR

#	Eligibility Criteria/Clause	Supporting Documents
	3. Cloud Access Security broker (CASB) with minimum 100 Licenses each Note: Experience should be during the five-year period preceding the RFP publication date. Even if the installation was completed more than five years ago, it will still qualify, provided the product is currently under maintenance or has been maintained at any time during the five-year period preceding the RFP publication date	A client-signed implementation report or official sign-off confirming the work OR Self-Declaration from OEM confirming the product & stage of the project and reference to the PO”
21	Compliance with the FRS, TRS, SoW, SBOM & CBOM Solution List: 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. SSL Orchestrator along with packet broker 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network/Anti-APT 6. Zero Trust Network Access (ZTNA) 7. Data Loss Prevention (DLP) 8. Information/Digital Right Management 9. Database Activity Monitoring 10. Mobile SDK 11. Host IPS including Application Change Control (HIPS) 12. Web Application Firewall (WAF) 13. Centralized key management solution 14. Certificate Lifecycle management 15. Identity & Access Management Solution 16. Multi Factor Authentication 17. Privilege Identity/Access Management 18. DNS Security Services (Internet-Facing DNS Security Services) 19. Cloud Access Security broker (CASB) 20. AI Security 21. SBOM, CBOM, AIBOM & QBOM	Self-declaration, in the format Annexure 18, from the respective OEM for each of the products & services proposed on their letterhead signed by the authorized signatory

#	Eligibility Criteria/Clause	Supporting Documents
22	Functional Compliance: The Bidder's proposed solution shall be evaluated for functional compliance against the requirements specified in Appendix 1A: Functional Compliance Sheet. The proposed product should have minimum functional compliance score of 85% for each of the following: 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. SSL Orchestrator along with packet broker 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network 6. Zero Trust Network Access (ZTNA) 7. Data Loss Prevention (DLP) 8. Information/Digital Right Management 9. Database Activity Monitoring 10. Mobile SDK 11. Host IPS including Application Change Control (HIPS) 12. Web Application Firewall (WAF) 13. Centralized key management solution 14. Certificate Lifecycle management 15. Identity & Access Management Solution 16. Multi Factor Authentication 17. Privilege Identity/Access Management 18. DNS Security Services (Internet-Facing DNS Security Services) 19. Cloud Access Security broker (CASB) 20. AI Security 21. SBOM, CBOM, AIBOM & QBOM	a) OEM Self Declaration b) Filled Appendix 1A: Functional Compliance c) Supporting Documentation like datasheets, product manuals, OEM website product feature listings etc.

#	Eligibility Criteria/Clause		Supporting Documents
	Each product/solution shall be evaluated independently, and the compliance score shall be computed separately for each product/solution.		
	Maximum Marks	Compliance (S/C)	Maximum Mark
	10	S (Standard):	This indicates that the requirement is covered by the standard product functionality. It includes features available out-of-the-box, as well as those achievable through parametrization or rules configuration.
	3	C (Customization):	Requirements marked as "C" are the ones that require minor modifications to the proposed solution. - Such customizations may include development of custom code, creation of new interfaces, user interface enhancements, or custom-built screens integrated with the base product. - All identified customizations shall be completed, tested, and made available by the bidder prior to commencement of User Acceptance Testing (UAT) (i.e, within 17 weeks of acceptance of PO), without impacting the Bank's project timelines.

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

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

- Attested copies of all relevant documents, certificates, work orders, completion certificates, financial statements, and other supporting documents shall be submitted as documentary evidence in support of the claims made by the bidder. The bidder shall furnish any additional information and clarification as may be required by the Bank for verification of eligibility criteria. The Bank reserves the right to independently verify, evaluate, and validate the information and claims submitted by the bidder. The decision of the Bank in this regard shall be final, conclusive, and binding on the bidder.
- In the event of a business transfer, acquisition, slump sale, merger, or acquisition of a business undertaking, the work experience, credentials, and references of the transferor entity ("Seller") pertaining to the acquired business may be considered, subject to submission of documentary evidence establishing such transfer and continuity of business operations.
- In cases involving corporate restructuring, including merger, amalgamation, demerger, name change, conversion, or reorganization, the incorporation certificate, financial statements, work experience credentials, technical qualifications, and other relevant records of the predecessor entity may be considered, subject to submission of documentary evidence acceptable to the Bank.
- Either the Principal/OEM or its authorized agent may submit a bid for a given item/product under this RFP. However, both the Principal/OEM and its authorized agent shall not be permitted to submit bids simultaneously for the same item/product in the same RFP. Further, where an agent is authorized to represent a Principal/OEM, the same agent shall not submit bids on behalf of more than one Principal/OEM for the same item/product under this RFP. Any violation of the above conditions shall render all such bids liable for rejection at the sole discretion of the Bank.

- e. The bidder and/or OEM shall comply with applicable guidelines issued by the Central Vigilance Commission (CVC), including Circular No. 03/01/12, the applicable provisions of the General Financial Rules (GFR), and the Department of Expenditure Office Memorandum dated 25.07.2016, as amended from time to time.
- f. In a tender, either the Indian Agent on behalf of the Principal/OEM or the Principal/OEM itself may bid; however, both shall not bid simultaneously for the same item/product in the same tender.
- g. Documentary evidence shall be furnished against each eligibility criterion along with a detailed index of documents submitted. All documents shall be duly signed and stamped by the Authorized Signatory of the bidder. Relevant sections of the submitted documents supporting compliance with the eligibility criteria shall be clearly highlighted for ease of verification by the Bank.
- h. Any misrepresentation, suppression of facts, submission of forged/fabricated documents, or provision of incorrect information by the bidder at any stage of the bidding process may result in rejection of the bid, forfeiture of bid security (if applicable), and/or blacklisting/debarment from participating in future procurement processes of the Bank, without prejudice to any other rights and remedies available to the Bank under law.
- i. For the purpose of this RFP, the term "Scheduled Bank" shall exclude Regional Rural Banks (RRBs) and Payment banks. Accordingly, experience shall be considered for the purpose of evaluating eligibility and qualification criteria under this RFP.
- j. Deployments shall be considered valid only if the solution has been used for its intended function in a production environment. Tests, pilot, or non-production deployments shall not be accepted.
- k. Experience of solution(s) can be shown in single /multiple Clients/work orders meeting the criteria(s)
- l. Experience should be during the five-year period preceding the RFP publication date. Even if the installation was completed more than five years ago, it will still qualify, provided the product is currently under maintenance or has been maintained at any time during the five-year period preceding the RFP publication date
- m. Experience must be showcased separately for each solution category, with clear evidence that each solution has been deployed as a standalone solution and not merely as a feature or component of another solution.
- n. When deemed necessary the Evaluation Committee may seek clarification on relevant aspects from the Bidder. However, that would not entitle the Bidder to change or cause any change.
- o. Bank reserves the right to conduct reference site visit/ video conference/ voice call with the Client to substantiate the credentials/ copy of PO/ Contract copy/ sign-off submitted by Bidder and/ or OEM. In case the input/ feedback received from the Customer is negative/ unsatisfactory, bank reserves the right to reject the Bid.

10.3 Technical Evaluation Criteria

Only those bidders who are found to be responsive and who meet all the Pre-Qualification (PQ) Criteria of the RFP, as determined by the Bank, shall be invited to give a Technical Presentation before the Bank's Evaluation Committee. The Technical Presentation shall form an integral part of the bid evaluation.

The Bank shall conduct a Technical Presentation of the proposed solution as part of the Evaluation process and shall be conducted only for the purpose of evaluating the bidder's proposed technical solution, architecture, infrastructure sizing, implementation methodology, operational approach, OEM capabilities, and compliance with the requirements of the RFP.

The date, time, venue, duration, and schedule of the Technical Presentation shall be communicated separately by the Bank to the eligible bidders. The Bank reserves the right to conduct the Technical Presentation in physical, virtual, or hybrid mode.

The Technical Presentation shall be made only by the bidder's proposed implementation team (Proposed Implementation Project Manager and Business Analyst, name of which should be part of the proposal complying with the requirement mentioned in the RFP) and/or respective OEM technical experts.

Only those bidders who secure the minimum qualifying marks prescribed by the Bank in the Technical Presentation shall be declared Technically Qualified.

Only the Commercial Bids of the Technically Qualified Bidders shall be opened and considered for Commercial Bid Evaluation. The minimum qualifying marks in the Technical Presentation shall be 80 out of 100 marks, unless otherwise specified by the Bank through the RFP or subsequent addendum.

The decision of the Bank regarding the evaluation of the Technical Presentation, award of marks, determination of technical qualification, and eligibility for Commercial Bid Evaluation shall be final and binding on all bidders

Evaluation Parameter	Detailed Sub-Parameters
1. Solution Understanding & Compliance (5 Marks)	- Understanding of the Bank's environment and proposed solution mapping. - Compliance with all requirements of the RFP. - Mapping of each RFP requirements to the proposed solution.
2. Technical Architecture & Solution Design (25 Marks)	- Overall architecture and logical design. - High Availability (HA) architecture for DC and DR. - Scalability to support future growth without redesign. - Component redundancy and elimination of single points of failure. - Integration architecture with bank's security applications - Network architecture including segmentation and communication flows - Logging and monitoring architecture.

Evaluation Parameter	Detailed Sub-Parameters
3. Implementation & Migration Methodology (25 Marks)	• Backup and disaster recovery architecture. • Project implementation methodology. • Deployment strategy. • Detailed implementation schedule with milestones. • OEM and Bidder's Resource deployment plan. • Installation methodology. • Configuration methodology. • Integration methodology. • Migration strategy. • Data migration methodology. • Cutover methodology. • Rollback strategy. • Testing methodology (FAT/SAT/SIT/UAT/PAT). • Risk identification and mitigation plan • Issue management process • Documentation deliverables. • Knowledge transfer methodology • Acceptance criteria. • Go-live support approach. • Post implementation stabilization plan.
4. Operations, Managed Services & SLA (10 Marks)	• Proposed operating model. • Roles and responsibilities of bidder, OEM and Bank. • Incident management process. • Service request management. • Preventive maintenance approach. • Health check methodology. • Performance monitoring methodology • Security monitoring process. • SLA monitoring mechanism. • Reporting and dashboard capabilities • Business continuity during maintenance. • Patch and upgrade management methodology.
5. OEM Support Model & TAC Availability (5 Marks)	• OEM support model throughout the contract period. • Availability of OEM TAC (24×7×365). • Support coverage for software, hardware and firmware. • Escalation process to OEM. • Local support availability. • Remote support capability. • Product lifecycle and end-of-support commitment. • Security patch release process. • Emergency support process.

Evaluation Parameter	Detailed Sub-Parameters
6. Project Management, Team & Certifications (5 Marks)	• OEM-backed support commitment. • Proposed project governance model. • Roles and responsibilities of each resource. • Resource deployment plan. • Backup resource plan. • Relevant OEM certifications. • Reporting and governance mechanism.
7. Sizing – IT Infrastructure (15 Marks)	• Compute sizing methodology. • CPU sizing justification. • Memory sizing justification. • Storage sizing methodology. • IOPS calculations. • Network bandwidth calculations. • Backup sizing. • Database sizing. • Virtualization sizing. • High Availability sizing. • DR sizing. • Future growth assumptions. • Infrastructure Bill of Materials mapping. • Virtual-to-Physical mapping. • Resource utilization assumptions.
8. Experience of Proposed OEMs (10 Marks)	• Support centre in India Locations and Support Personnel's • Number of enterprise deployments. • Number of BFSI deployments. • Number of deployments in India. • Number of deployments of similar scale. • Support commitment during contract period • Availability of local OEM office.

10.4 Commercial Evaluation Criteria

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

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

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

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

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

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

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

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

Commercial Bid Evaluation Considerations:

Commercial bid valuation shall be considered as below in case of any kind of discrepancy:

1. Hardware Cost:

- The Bidder shall be solely responsible for sizing the IT Infrastructure required to meet all functional, technical, performance, scalability, availability, security, retention, and SLA requirements specified under the RFP and shall submit the same through the Masked BoM.
- If, during technical evaluation, the Bank observes that the proposed sizing is inadequate, undersized, or requires augmentation, the Bidder shall revise the sizing and update the Masked BoM accordingly. However, such review or technical acceptance by the Bank shall not dilute the Bidder's sole ownership and responsibility for the correctness, adequacy, and completeness of the sizing. The Bank's review, observations, clarification requests, technical acceptance, or failure to identify any

deficiency during the evaluation process shall not be construed as validation of the sizing proposed by the Bidder, nor shall it relieve the Bidder of its sole and absolute responsibility for the correctness, adequacy, completeness, and fitness of the sizing to meet all requirements of the RFP.

- Notwithstanding the Bank's technical acceptance of the sizing, the Bidder shall remain fully responsible for ensuring compliance with all RFP requirements throughout the Contract Period. Any subsequent augmentation, upgrade, replacement, or addition of infrastructure components required due to incorrect sizing, underestimation, inadequate capacity planning, or failure to meet the prescribed requirements and SLAs shall be carried out by the Bidder at no additional cost to the Bank, unless otherwise approved by the Bank in writing.
- 2. If there is a discrepancy between words and figures, the amount in words shall prevail
- 3. If there is a discrepancy between percentage and amount, the amount calculated as per the stipulated percentage basis shall prevail
- 4. Where there is a discrepancy between the unit rate and the line-item total resulting from multiplying the unit rate by quantity, the unit rate will govern unless, in the opinion of bank, there is an obvious error such as a misplacement of a decimal point, in which case the line-item total will prevail
- 5. Where there is a discrepancy between the amount mentioned in the bid and the total line-item present in the schedule of prices, the amount obtained on totaling the line items in the Bill of Materials will prevail
- 6. The amount stated in the correction form, adjusted in accordance with the above procedure, shall be considered as binding, unless it causes the overall price to rise, in which case the bid price shall prevail
- 7. If there is a discrepancy in the total, the correct total shall be arrived at by bank.
- 8. In case the bidder does not accept the correction of the errors as stated above, the bid shall be rejected.
- 9. At the sole discretion and determination of the bank, the bank may add any other relevant criteria for evaluating the proposals received in response to this RFP.
- 10. Bank may, at its sole discretion, decide to seek more information from the respondents in order to normalize the bids. However, respondents will be notified separately if such normalization exercise as part of the technical evaluation is resorted to.
- 11. All liability related to non-compliance of minimum wages requirement and any other law will be responsibility of the bidder.
- 12. The bank shall not incur any liability to the affected bidder on account of such rejection.
- 13. The commercials will be calculated till two decimal points only. If the third decimal point is greater than .005 the same shall be scaled up else, it shall be scaled down to arrive at two decimal points. Bank will make similar treatment for 4th or subsequent decimal point to finally arrive at two decimal points only.

11 PAYMENT TERMS

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

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

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

11.1 Product (Software) Cost

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

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

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

Note:

- The payment milestones specified under Product License Cost and Subscription Cost shall be applicable to the respective licensing model proposed by the bidder.
- Irrespective of whether the bidder proposes a Perpetual Licensing Model, Subscription Licensing Model, or any other OEM-supported licensing model, the quoted Product License Cost/Subscription Cost, as applicable, shall include the applicable software licence/subscription together with three (3) years of OEM warranty, support, updates, upgrades, patches, bug fixes, and maintenance, in accordance with Section 7.9 (Warranty, ATS & AMC) and other provisions of the RFP.
- For Perpetual or any other non-subscription licensing model, the Annual Technical Support (ATS) charges for Year-4 and Year-5 shall be quoted separately in the Commercial Bill of Material and shall be payable from the fourth year onwards.
- For the Subscription Licensing Model, the Subscription Renewal Charges for Year-4 and Year-5 shall be quoted separately in the Commercial Bill of Material and shall be payable from the fourth year onwards.
- Accordingly, the payment milestones and the Commercial Bill of Material prescribed in the RFP are applicable to all licensing models.

11.2 OEM Services Cost

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

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

11.3 Hardware Cost

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

S. No.	Items	Milestone	Percentage
1	Appliance Cost	On successful Delivery of the Appliance which would be considered delivered once the solution (with OOTB features) is made available for view and review of the bank.	50%
		The Bidder is required to submit the required to submit the following: • Delivery proof • OOTB Installation Proof • Invoice of the Product	
		On successful UAT Signoff of the respective product	20%
		On successful Go-live of the respective product	30%
2.	Hardware Cost (Other	Delivery (power on) of hardware and submission of invoice with Proof of Delivery and other documents of the hardware	70%

S. No.	Items	Milestone	Percentage
	than Appliances)	supplied. Bank may at its discretion verify the details before releasing the payment (This verification, if required, shall be completed within 1 month of delivery of the hardware on the bank's premises).	
		On successful installation of proposed solutions on the hardware - 50% of the sought product/solutions	15%
		On successful installation of remaining proposed solution on the hardware – remaining 50% of the sought product/solutions	15%

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

11.4 ATS/subscription cost & AMC Cost

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

S. No	Items	Milestone	Percentage
1	ATS/ Annual Subscription & Appliance AMC Cost	ATS/ Annual Subscription Cost	Yearly in advance (Post submission of 110% of Annual subscription cost in the form of Bank Guarantee of the respective product) or quarterly in arrears
		Appliance AMC	Yearly in advance (Post submission of 110% of the yearly AMC Amount of the respective product in the form bank guarantee) or quarterly in arrears

11.5 Facility Management (FM) Cost:

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

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

11.6 Other Cost

Cost for the respective line items in the Bill of Material

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

Note:

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

12 SERVICE LEVELS & PENALTIES

12.1 Service Level Agreement

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

1. The successful bidder shall enter into a **Service Level Agreement (SLA)** incorporating all applicable terms and conditions of this RFP for maintaining the required uptime and providing support services, including onsite support, throughout the contract period.
2. The bidder and the OEM shall be jointly responsible for the maintenance, configuration, performance, and fault-free operation of the entire supplied infrastructure, including hardware, software, operating systems, databases, and related components, during the warranty, AMC, ATS, and FMS periods, as applicable.
3. Any technical issues, faults, or malfunction affecting the installed solution, including bidder's provided hardware, software, operating systems, databases, firmware, BIOS, or related components, shall be attended to on a priority basis and shall be covered under the applicable warranty, AMC, ATS, and FMS.
4. The bidder should maintain the guaranteed minimum uptime for all systems and solutions supplied under this RFP to prevent business disruption, service degradation, or data unavailability. Uptime shall be measured and calculated on a monthly basis.
5. Incidents, faults, or breakdowns may be reported by the Bank through telephone, email, service desk ticketing system, or any other mutually agreed communication mechanism.
6. For SLA and penalty calculations, downtime shall be measured from the time the Bank/bank's appointed vendor reports the incident to the bidder until the time the bidder notifies the Bank that the issue has been resolved, and normal services have been restored, subject to verification by the Bank.
7. Any applicable penalties shall be deducted from the quarterly AMC, ATS, or FMS payments. If the penalty amount cannot be recovered through such payments, the Bank reserves the right to recover the amount by invoking the Performance Bank Guarantee (PBG).
8. Failure to provide support services in accordance with the SLA requirements, including the required support coverage and service quality specified in this RFP, may result in bank levying penalty, termination of the contract, or any other action deemed appropriate by the Bank, without prejudice to its other contractual rights and remedies.
9. The bidder shall conduct preventive maintenance activities at least once every quarter and perform breakdown maintenance as required, without adversely affecting the Bank's normal operations. Such activities shall support the maintenance of the required up-time on a 24x7x365 basis.
10. The Bank's normal business hours are from **09:00 AM to 6:00 PM** on operational branch working days. However, the bidder shall provide support services on a **24x7x365 basis** and, whenever required, perform activities beyond normal business hours, including weekends and holidays

11. In addition to maintaining the required uptime, the bidder shall adhere to the incident response, restoration, and resolution timelines specified in this RFP for all hardware, software, system software, and related component failures
12. Uptime shall be calculated as follows:

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

Planned or scheduled downtime approved in advance by the Bank shall be excluded from uptime and penalty calculations. The Bank shall make payments after deducting any applicable LD & SLA penalties.
13. If any critical component of the supplied solution becomes non-functional, the bidder and OEM shall, within **four (4) hours** of incident reporting, either:
 - a) repair the defective component,
 - b) replace it with a new equivalent component, or
 - c) provide a standby replacement at no additional cost to the Bank.

The bidder shall maintain adequate inventory of spare and standby components to meet this requirement
14. If the bidder fails to restore service or provide a replacement/standby component within the stipulated four (4) hour period, the Bank may undertake or arrange remedial measures at the bidder's risk and cost, without prejudice to any other rights and remedies available under the contract.
15. The bidder shall comply with the Bank's security policies, audit requirements, and applicable regulatory guidelines. The bidder shall also implement all necessary operating system, firmware, BIOS, security, and related updates or patches during the contract period at no additional cost to the Bank.
16. If any customer-facing application, Core Banking System (CBS), regulatory application, statutory application, or other critical banking service becomes unavailable, disrupted, or degraded due to an issue attributable to the Core Firewall or Perimeter Firewall or solution(s) supplied under this RFP, and the incident is classified by the Bank as a **Critical-Level Incident**, the Bank may impose an additional penalty over and above the standard SLA penalties. Where such an incident remains unresolved for more than **120 minutes**, an additional penalty of **0.5% of the monthly maintenance charges** shall be levied for every subsequent hour or part thereof until the issue is resolved and normal services are restored.
17. For all incidents related to the supplied solution, the bidder shall submit a **Root Cause Analysis (RCA)** report issued by the respective OEM within **three (3) working days** from the date of incident resolution. A penalty of **₹20,000 per calendar day** shall be levied for any delay in submission of the RCA report beyond the defined timelines.
18. The Bank shall not levy multiple penalties for the same event, incident, delay, or service deficiency. In case multiple penalty provisions are applicable, only the highest applicable penalty shall be levied.
19. Total penalties due Service level and liquidated damages shall not exceed 10% of the Total contract value.

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

Level Classifications

CRITICALITY TABLE

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

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

Service Levels

1. Service Level monitoring shall include both **Availability Metrics** and **Performance Metrics** for all solutions, infrastructure, software, appliances, and services supplied under this RFP.
2. The bidder shall submit **Monthly Availability Reports** and **Quarterly Availability Reports** to the Bank. These reports shall be reviewed by the Bank to assess compliance with the agreed Service Levels.
3. The Monthly Availability Report shall be submitted within the timelines specified by the Bank and shall, at a minimum, include:
 - a. System and service availability statistics;

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

- c. The bidder shall provide the Bank with access to relevant tools, dashboards, logs, and reports required to independently verify SLA compliance and service performance.
- d. The Bank reserves the right to validate, audit, or independently measure the Service Levels through its own tools, processes, or authorized third-party agencies. In the event of any discrepancy, the Bank's determination shall prevail unless the bidder provides satisfactory evidence to the contrary.

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

Monthly Maintenance Cost =	$\frac{\text{Total FM (O\&M) Manpower Cost} + \text{Total AMC Cost of Infrastructure/Appliances} + \text{Total ATS or Subscription Cost of Software/Tools}}{60}$
----------------------------	--

Quarterly Maintenance Cost =	$\frac{\text{Total FM (O\&M) Manpower Cost} + \text{Total AMC Cost of Infrastructure/Appliances} + \text{Total ATS or Subscription Cost of Software/Tools}}{20}$
------------------------------	--

Availability Measurements

Level	Type of Infrastructure	Measurement	Minimum Service Level	Penalty
Cyber Security Solutions listed below, including security appliances, software, databases, licenses, subscriptions, and all components supplied, implemented, and managed by the bidder under this RFP List of solutions: 1. Anti-Distributed Denial of Services (Anti-DDoS)	Proposed Infrastructure & Systems	Availability of each solution, Infrastructure Elements & Systems, any individual component	99.99%	For every 0.01% reduction, or part thereof, below the prescribed availability level of 99.99%, a penalty equivalent to 1% of the Monthly Maintenance Cost (MMC) shall be levied

Level	Type of Infrastructure	Measurement	Minimum Service Level	Penalty
2. SSL Orchestrator along with packet broker 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network 6. Zero Trust Network Access (ZTNA) 7. Data Loss Prevention (DLP) 8. Information/Digital Right Management 9. Database Activity Monitoring 10. Mobile SDK 11. Host IPS including Application Change Control (HIPS) 12. Web Application Firewall (WAF) 13. Centralized key management solution 14. Certificate Lifecycle management 15. Identity & Access Management Solution 16. Multi Factor Authentication 17. Privilege Identity/Access Management				

Level	Type of Infrastructure	Measurement	Minimum Service Level	Penalty
18. DNS Security Services (Internet-Facing DNS Security Services) 19. Cloud Access Security broker (CASB) 20. AI Security				
Cyber Security Solutions listed below , including security appliances, software, databases, licenses, subscriptions, and all components supplied, implemented, and managed by the bidder under this RFP List of solutions: 21. SBOM/CBOM/AIBOM/QBOM	Proposed Infrastructure & Systems	Availability of each solution, Infrastructure Elements & Systems, any individual component	99.50%	For every 0.01% reduction, or part thereof, below the prescribed availability level of 99.50%, a penalty equivalent to 1% of the Monthly Maintenance Cost (MMC) shall be levied

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

Performance Measurements

Performance measurements should be conducted on a **monthly basis** and may also be carried out at any other time as reasonably required by the Bank.

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

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

Incident Management

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

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

Management, Reporting and Governance

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

Service Level	Description	Measurement Method	Periodicity	MSL	Service Credit / Penalty	Remarks
	acceptable to the Bank.					
Manpower Availability	The bidder shall maintain the minimum manpower strength specified in the RFP at all times. Any absence shall be immediately substituted with an equivalent or higher skilled resource.	Actual manpower deployed ÷ Required manpower strength × 100.	Monthly	100%	Any breach of the 100% availability requirement for the mandatory minimum positions and resource counts specified in the RFP shall attract a penalty of INR 25,000 per resource per week or part thereof Penalty shall be applicable from the date of breach until the required manpower strength is restored. The mandatory minimum positions specified under Section 7.10 (Resource Requirement – Minimum Resource Count Deployment) shall be maintained at 100% throughout the Contract Period. Any	Resource availability shall be calculated monthly based on approved attendance records and deployment reports.

Service Level	Description	Measurement Method	Periodicity	MSL	Service Credit / Penalty	Remarks
					vacancy, absence, or shortfall in the mandatory minimum resource count shall be immediately replaced with an equivalent or higher-skilled resource. Failure to maintain the mandatory minimum deployment shall be considered an SLA breach and shall attract penalties as defined below from the date of breach until the required deployment is restored.	
SLA and Operational Report Submission	The bidder shall submit all SLA, performance, operational, compliance and governance reports as prescribed by the Bank.	Number of reports submitted within stipulated timelines ÷ Total reports due.	Monthly	100%	Penalty of INR 20,000 per week or part thereof for each delayed or missed report.	All reports for a calendar month shall be submitted by the 7th day of the subsequent month unless otherwise specified by the Bank. The Bank may modify the reporting requirements during the contract period.
Security Device Management	The bidder shall provide 24x7 monitoring,	Number of approved changes	Monthly	100%	Incorrect rule/configuration	Applies to all security devices and solutions covered under the scope of the RFP. All changes

Service Level	Description	Measurement Method	Periodicity	MSL	Service Credit / Penalty	Remarks
and Administration	management, administration, configuration and change management services for all in-scope security solutions and devices.	executed without error ÷ Total approved changes implemented.			change: INR 20,000 per instance. Incorrect rule/configuration change resulting in service disruption, security incident, or business impact: INR 30,000 per instance.	shall be implemented only after obtaining requisite approvals from the Bank.

Security Vulnerability Management:

Service Area	Service Level Description	Measurement Method	Periodicity	MSL	Service Credit / Penalty
Version Upgrades, Security Patching and Firmware Updates	The bidder shall implement all OEM-recommended and Bank-approved operating system, database, middleware, application, firmware, security, and hardware patches/upgrades in accordance with the approved Patch and Upgrade Management Calendar. The bidder shall publish a monthly patching and upgrade schedule and obtain necessary approvals prior to implementation. This SLA shall become applicable one (1) month after Go-Live/Operational Acceptance.	Number of approved upgrades, patches, firmware updates and version updates successfully implemented within the approved timeline ÷ Total upgrades, patches, firmware updates and version updates due during the measurement period × 100.	Monthly	95%	95% and above compliance: No Penalty. Below 95% compliance: Penalty of INR 500 per day per percentage point (or part thereof) below the prescribed MSL, until the pending upgrades/patches are successfully implemented and verified by the Bank.

Management & health checkup:

Service Area	Service Level Description	Measurement Method	Periodicity	MSL	Service Credit / Penalty
OEM Governance and Review	The bidder shall ensure participation of the respective OEM(s) in periodic review meetings, health checks, architecture reviews, performance reviews, and issue resolution discussions as required by the Bank and specified in the RFP.	Number of OEM review engagements conducted as scheduled ÷ Number of OEM review engagements required.	As Required	100%	Failure to conduct the scheduled OEM review or engagement shall attract a penalty of INR 2,00,000 per affected solution per day or part thereof from the scheduled date of the review until completion of the OEM engagement.
OEM Support Case Management	The bidder shall proactively manage and coordinate with OEMs for resolution of product defects, bugs, vulnerabilities, and technical issues. All OEM support tickets shall be tracked and escalated appropriately until closure or implementation of an acceptable workaround approved by the Bank.	Number of OEM support cases resolved within the prescribed timeline ÷ Total OEM support cases due for closure.	Monthly	100%	For OEM support cases remaining unresolved beyond 14 calendar days without a Bank-approved workaround, penalty of 1% of the applicable monthly ATS/AMC/Managed Services charges per week or part thereof until closure.
Compliance with RBI, CERT-In and Regulatory Advisories	The bidder shall assess, implement and ensure compliance with all applicable RBI, CERT-In, Government of India, regulatory, statutory, and security advisories	Number of applicable advisories complied with within prescribed timelines ÷ Total applicable advisories.	Monthly	100%	Compliance within the stipulated timeline – No Penalty. Delay in compliance beyond the prescribed due date shall attract a

Service Area	Service Level Description	Measurement Method	Periodicity	MSL	Service Credit / Penalty
	within the timelines prescribed by the issuing authority or as directed by the Bank.				penalty of 0.5% of the applicable monthly contract value per day of delay, subject to the overall penalty cap specified in the RFP.

Audit (IS & VAPT and other internal/external audit) Gaps

Service Area	Observation Severity	Resolution Timeline	Service Requirement	Level	Penalty
IS Audit / VAPT / Security Audit Observation Closure	Highly Critical	Within 24 hours from identification of the vulnerability	100% closure within prescribed timeline		INR 50,000 per observation per 6 hours or part thereof beyond the prescribed timeline until closure and acceptance by the Bank.
	Critical	Within 15 calendar days from issuance of the audit report or identification of the vulnerability	100% closure within prescribed timeline		INR 20,000 per observation per day or part thereof beyond the prescribed timeline until closure and acceptance by the Bank.
	High	Within 30 calendar days from issuance of the audit report or identification of the vulnerability	100% closure within prescribed timeline		INR 10,000 per observation per day or part thereof beyond the prescribed timeline until closure and acceptance by the Bank.
	Medium	Within 45 calendar days from issuance of the audit report or identification of the vulnerability	100% closure within prescribed timeline		INR 5,000 per observation per day or part thereof beyond the prescribed timeline until closure and acceptance by the Bank.
	Low	Within 60 calendar days from issuance of the audit report or	100% closure within prescribed timeline		INR 3,000 per observation per day or part thereof beyond the prescribed timeline until closure and acceptance by the Bank.

Service Area	Observation Severity	Resolution Timeline	Service Requirement	Level	Penalty
		identification of the vulnerability			

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

12.2 Penalties

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

Liquidated Damages

Supply & Delivery

Please refer to section 13.19 for LD on Supply & Delivery

Installation & Implementation

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

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

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

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

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

12.3 At-Risk Amount

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

13 TERMS AND CONDITIONS

13.1 Assignment & Subcontracting

1. The selected bidder shall not subcontract/JV/Consortium or permit anyone to perform any of the work, service or other performance required under the contract (excluding Proposed OEM personnels). All bidder's personnel proposed for the bank shall be on bidder's Payroll. Bank will seek relevant documentation from the bidder to validate the same.
2. The Bidder shall not undergo any merger, amalgamation, acquisition, change in control, transfer of substantial ownership or restructuring which materially affects its ability to perform the Contract without prior written intimation to and, where considered necessary by the Bank, prior written approval of the Bank. Any such change which, in the reasonable opinion of the Bank, adversely affects the Bidder's capability, financial standing, security posture or contractual performance shall constitute a ground for termination
3. If the Bank undergoes a merger, amalgamation, takeover, consolidation, reconstruction, change of ownership, etc., this tender shall be assigned to the new entity, and such an act shall not affect the rights of the Agency under this tender.

13.2 Right to Alter quantities

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

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

13.3 Delays in the Bidder's Performance

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

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

The remedies available to the Bank for delay shall be cumulative and shall be without prejudice to the Bank's other contractual, statutory or legal rights and remedies, including recovery of losses/costs, invocation of PBG, termination and procurement from alternative sources.

13.4 Jurisdiction

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

13.5 Dispute Resolution

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

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

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

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

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

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

13.6 Notices

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

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

Publicity

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

13.7 Legal Compliance

The successful bidder hereto agrees that it shall comply with all applicable union, state and local laws, ordinances, regulations and codes in performing its obligations hereunder, including the procurement of licenses, permits and certificates and payment of taxes where required. The Successful bidder shall maintain all proper records, particularly but without limitation accounting records, required by any law, code, practice or corporate policy applicable to it from time to time including records, returns and applicable documents under the Labour Legislation

The Bidder shall comply with all applicable laws, rules, regulations, notifications, directions and guidelines issued by the Government of India, RBI, CERT-In, NPCI, CVC and other applicable statutory/regulatory authorities, as well as the Bank's applicable policies, standards and security requirements, as amended from time to time.

Any regulatory or statutory requirement becoming applicable during the Contract Period and relating to the services/systems covered under this RFP shall be implemented by the Bidder within the timelines prescribed by the Bank/regulator and, where such requirement relates to the contracted scope, without additional cost to the Bank

13.8 Digital Personal Data Protection Compliance

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

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

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

13.9 Non-Disclosure Agreement

The Service Provider shall take all necessary precautions to ensure that all confidential information is treated as confidential and not disclosed or used other than for the purpose of project execution. Service Provider shall suitably defend, indemnify Bank for any loss/damage suffered

by Bank. The Service Provider shall have to sign a Non-Disclosure Agreement on stamp paper. No media release, public announcement or any other reference to the agreement or any program there under shall be made without the written consent from the Bank. Reproduction of this agreement, without the prior written consent of the Bank, by photographic, electronic or other means is strictly prohibited.

13.10 Solicitation of Employees

Both parties agree not to hire, solicit, or accept solicitation (either directly, indirectly, or through a third party) for their employees directly involved in this contract during the period of the contract and one year thereafter, except as the parties may agree on a case-by-case basis. The parties agree that for the period of the contract and one year thereafter, neither party will cause or permit any of its directors or employees who have knowledge of the agreement to directly or indirectly solicit for employment the key personnel working on the project contemplated in this proposal except with the written consent of the other party. The above restriction would not apply to either party for hiring such key personnel who (i) initiate discussions regarding such employment without any direct or indirect solicitation by the other party (ii) respond to any public advertisement placed by either party or its affiliates in a publication of general circulation or (iii) has been terminated by a party prior to the commencement of employment discussions with the other party.

13.11 Authorized Signatory

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

13.12 Confidentiality

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

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

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

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

13.13 Indemnity

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

The Bidder shall indemnify, defend and hold harmless the Bank, its directors, officers, employees and representatives against all losses, damages, liabilities, claims, demands, actions, proceedings, penalties, costs and expenses (including reasonable legal expenses, forensic investigation costs, remediation costs and costs incurred in responding to regulatory/customer claims) arising out of or relating to:

- (a) breach of the Contract/RFP/SLA;
- (b) negligence, gross negligence, fraud, willful misconduct or omission of the Bidder/OEM/subcontractor;
- (c) breach of confidentiality or data protection obligations;
- (d) cyber security incident, data breach, unauthorised access, loss or disclosure of Bank/customer data attributable to the Bidder/OEM/subcontractor;
- (e) infringement of intellectual property rights;
- (f) violation of applicable law, regulatory directions or statutory requirements attributable to the Bidder/OEM/subcontractor;
- (g) third-party/customer claims arising from the acts or omissions of the Bidder/OEM/subcontractor; and
- (h) any loss suffered by the Bank in consequence of failure of the Bidder to perform the services in accordance with the Contract.

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

The indemnity obligations shall be independent of and in addition to the Bank's rights relating to liquidated damages, SLA penalties, service credits, recovery, set-off, PBG invocation and termination.

13.14 Make in India

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

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

13.15 Force Majeure

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

- Natural phenomenon, including but not limited to floods, droughts, earthquakes, epidemics and pandemics
- Acts of any government, including but not limited to war, declared or undeclared priorities, quarantines and embargos
- Terrorist attack, public unrest in work area
- Provided either party shall within 10 days from occurrence of such a cause, notify the other in writing of such causes. The Bidder or The Bank shall not be liable for delay in performing his/her obligations resulting from any force Majeure cause as referred to and/or defined above. Any delay beyond 30 days shall lead to termination of contract by parties and all obligations expressed quantitatively shall be calculated as on date of termination. Notwithstanding this, provisions related to indemnity, confidentiality survive termination of the contract.
- Unless otherwise directed by the bank in writing, the Bidder affected by force majeure shall continue to perform the obligations under this agreement, which are not affected by the force majeure event and shall take such steps as are reasonably necessary to remove the causes resulting in force majeure and to mitigate the effect thereof.
- As soon as the cause of force majeure has been removed, the Bidder shall notify the Bank and resume the affected activity without delay.
- Notwithstanding the above, the decision of the bank shall be final and binding on the Bidder in the event of force majeure.

For avoidance of doubt, Force Majeure shall not include failure of the Bidder/OEM/subcontractor, shortage or unavailability of manpower, financial difficulties, failure of subcontractors or suppliers, failure to procure equipment/software/licenses, ordinary hardware/software failure, cyber-security vulnerabilities, malware/ransomware incidents attributable to inadequate security controls, or any event which could reasonably have been prevented, mitigated or overcome by the exercise of due diligence and reasonable business continuity measure

13.16 Ownership & Retention of Documents:

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

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

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

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

The expression ‘Documents’ shall include, without limitation, Bank Data, system configurations, security policies, rules, logs, audit trails, reports, dashboards, source/configuration files specifically developed for the Bank, credentials, certificates, encryption keys, documentation, manuals, SOPs, scripts, migration artefacts and other deliverables created or maintained in connection with the Contract. The Bidder shall not exercise any lien, right of retention or other encumbrance over any Bank Data, Documents or deliverables for any reason whatsoever.

13.17 Conflict of Interest:

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

13.18 Signing of Pre-Contract Integrity Pact:

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

13.19 Liquidated Damages

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

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

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

If the bidder fails to deliver any or all of the products and/or systems and/or services solutions within the time period(s) specified in the Delivery Schedule or installation, the Bank shall, without prejudice

to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 0.5 percent per week or part thereof of Contract Price subject to maximum deduction of 10% of the total contract value, until actual delivery, installation or performance as per related clauses mentioned in RFP.

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

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

13.20 Intellectual Property Indemnity:

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

Further, where continued use of the affected product/service is prohibited or reasonably likely to result in infringement, the Bidder shall, at its own cost and without disruption to the Bank's operations, either procure the necessary right/license, replace or modify the affected product/service with an equivalent or superior non-infringing solution, or refund the corresponding amounts paid by the Bank, without prejudice to the Bank's other rights and remedies.

13.21 Limitation of Liability

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

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

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

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

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

13.22 Order Cancellation

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

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

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

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

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

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

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

Bidder's Obligation on termination

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

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

13.23 Consequences of Termination

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

In the event that the termination of the Contract is due to the expiry of the term of the Contract, a decision not to grant any (further) extension by the Bank, the Bidder herein shall be obliged to provide all such assistance to the next successor Bidder or any other person as may be required and as The Bank may specify including training, where the successor(s) is a representative/personnel of The Bank to enable the successor to adequately provide the Service(s) hereunder, even where such assistance is required to be rendered for a reasonable period that may extend beyond the term/earlier termination

hereof. Nothing herein shall restrict the right of The Bank to invoke the Performance Bank Guarantee and other guarantees, securities furnished, enforce the Deed of Indemnity and pursue such other rights and/or remedies that may be available to The Bank under law or otherwise. The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the Contract that are expressly or by implication intended to come into or continue in force on or after such termination.

Notwithstanding the foregoing, the Bank shall be entitled to terminate the Contract, in whole or in part, with immediate effect and without any cure period where:

- a. there is a material cyber-security incident attributable to the Bidder;
- b. Bank/customer data is compromised, disclosed, lost or accessed without authorisation;
- c. there is fraud, wilful misconduct or gross negligence;
- d. confidentiality obligations are materially breached;
- e. the Bidder/OEM is blacklisted/debarred by a competent regulator/statutory authority;
- f. continued engagement is prohibited or restricted by RBI, Government or any competent regulatory authority;
- g. the Bidder becomes insolvent or enters liquidation;
- h. there is unauthorised assignment/subcontracting;
- i. material false representation or suppression of material information is discovered; or
- j. continuation of the services is, in the Bank's reasonable opinion, likely to adversely affect the Bank's information-security, regulatory or operational interests.

In case of termination for convenience, the Bidder shall not be entitled to claim loss of profit, loss of anticipated revenue, compensation for unexecuted portion, consequential damages or any other termination compensation. The Bank shall only be liable for undisputed amounts properly due for services actually and satisfactorily performed up to the effective date of termination.

Upon expiry or termination, the Bidder shall immediately cease all access to Bank systems except to the extent expressly authorised by the Bank for transition purposes.

The Bidder shall provide a certificate confirming return/deletion of Bank Data, credentials, keys and confidential information, subject to retention required by law or regulatory direction.

The Bidder shall not withhold any Bank Data, Documents, credentials, configurations, logs or deliverables on account of any payment dispute.

13.24 Audit by Third Party

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

Provider shall, whenever required by the Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by the Bank.

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

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

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

13.25 Access Through Virtual Private Network (VPN)

The Bank may, at its sole discretion, provide remote access to its information technology system to IT Service Provider through secured Virtual Private Network (VPN) to facilitate the performance of IT Services. Such remote access to the Bank's information technology system shall be subject to the following:

1. Service Provider shall ensure that the remote access to the Bank's VPN is performed through a laptop/desktop ("Device") specially allotted for that purpose by the Service Provider and not through any other private or public Device.
2. Service Provider shall ensure that only its authorized employees/representatives access the Device.
3. Service Provider shall be required to get the Device hardened/configured as per the Bank's prevailing standards and policy.
4. Service Provider and/or its employee/representative shall be required to furnish an undertaking and/or information security declaration on the Bank's prescribed format before such remote access is provided by the Bank.
5. Service Provider shall ensure that services are performed in a physically protected and secure environment which ensures confidentiality and integrity of the Bank's data and artifacts, including but not limited to information (on customer, account, transactions, users, usage, staff, etc.), architecture (information, data, network, application, security, etc.), programming codes, access configurations, parameter settings, executable files, etc., which the Bank representative may inspect. The service Provider shall facilitate and/ or handover the Device to the Bank or its authorized representative for investigation and/or forensic audit.

6. Service Provider shall be responsible for protecting its network and subnetworks, from which remote access to the Bank's network is performed, effectively against unauthorized access, malware, malicious code and other threats to ensure the Bank's information technology system is not compromised in the course of using remote access facility.

13.26 INSURANCE

The Bidder shall, throughout the Contract Period, maintain adequate insurance policies covering, as applicable, professional liability/errors and omissions, cyber liability/data breach, employee fidelity, third-party liability, workmen compensation and such other risks as may reasonably be required having regard to the nature of the services. The Bidder shall furnish copies of valid insurance policies/certificates to the Bank on demand. Maintenance of insurance shall not limit or reduce the Bidder's liability under the Contract."

13.27 SEVERABILITY

If any provision of the Contract is held to be invalid, illegal or unenforceable, the remaining provisions shall continue in full force and effect, and the parties shall endeavour to replace the affected provision with a valid provision which most closely reflects the original commercial and legal intent.

13.28 NO LIEN OVER BANK DATA

The Bidder shall have no lien, right of retention, security interest or other encumbrance over Bank Data, customer data, system configurations, logs, documents, credentials, source/configuration materials or other Bank assets, irrespective of any dispute regarding payment or performance.

14 APPENDIX

14.1 APPENDIX 1A: Functional Compliance Sheet:

Attached as a separate Excel file.

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

14.2 APPENDIX 1B: Technical Compliance Sheet:

Attached as a separate Excel file.

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

14.3 APPENDIX 2: Commercial Bill of material Sheet

Attached as a separate Excel file.

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

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

Attached as a separate Excel file.

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

15 ANNEXURES

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

S.No.	Particulars	Submitted (Yes/No)	Page No
1	Bidder's Information		
2	Tender Covering Letter		
3	Bid Security Declaration		
4	Pre-Qualification Criteria		
5	Acceptance/Compliance Certificate		
6	Manufacturer's Authorization form		
7	Certification on OEM requirement		
8	Escalation matrix		
9	Litigation Certificate		
10	Non- Blacklisting undertaking		
11	Undertaking of Authenticity		
12	Non-Disclosure agreement		
13	Commercial proposal submission checklist		
14	Bank guarantee format for EMD		
15	Format for Performance guarantee		
16	Pre-contract integrity pact		
17	Compliance with FRS, TRS, SoW & SBOM		
18	Stack Confirmation Sheet		
19	S-BOM & C-BOM Details of all the proposed Tool/solutions		
20	Technical Presentation Submission		
21	Signed Copy of RFP		
22	Signed Copy of Corrigendum, if any		
23	Appendix 1A, Appendix 3 & Masked Appendix 2		

Note:

- a) All pages of the bid documents must be sealed & signed in full by authorized person.
- b) All pages of the bid documents should be numbered in serial order i.e. 1, 2, 3....
- c) Bank may ask for any other document on its discretion.

Signature & Seal of the Bidder

15.2 Annexure 2: Bidder's Information

Bidder's Information

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

Reg: Selection of Bidder for Supply Installation, Implementation, Maintenance & Management of

Ref: RFP No. _____ dated _____

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

Mobile No.	
Email Address	

Wherever applicable submit documentary evidence to facilitate verification.

DECLARATION:

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

1. The Bank is not bound to accept the lowest bid or may reject all or any bid at any stage at its sole discretion without assigning any reason, therefore.
2. If our Bid for the above job is accepted, we undertake to enter into and execute at our cost, when called upon by the Bank to do so, a contract in the prescribed form. Unless and until a formal contract is prepared and executed, this bid together with your written acceptance thereof shall constitute a binding contract between us.
3. We have read and understood all the terms and conditions and contents of the RFP and also undertake that our bid conforms to all the terms and conditions and does not contain any deviation and misrepresentation. We understand that the bank reserves the right to reject our bid on account of any misrepresentation/deviations contained in the bid.
4. Bank may accept or entrust the entire work to one Bidder or divide the work to more than one bidder without assigning any reason or giving any explanation whatsoever and the Bank's decision in this regard shall be final and binding on us.
5. I/ We do not have any conflict of interest as mentioned in the RFP document.
6. I/We submit this application under and in accordance with the terms of the RFP document and agree and undertake to abide by all the terms and conditions of the RFP document.
7. The Prices submitted by us have been arrived at without agreement with any other Bidder of this RFP for the purpose of restricting competition.
8. The prices submitted by us have not been disclosed and will not be disclosed to any other Bidder responding to this RFP.
9. We have not induced or attempted to induce any other Bidder to submit or not to submit a Bid for restricting competition.
10. We have quoted for all the services/items mentioned in this RFP in our price Bid.
11. The rate quoted in the price Bids are as per the RFP and subsequent pre-Bid clarifications/modifications/ revisions furnished by the Bank, without any exception.
12. We agree to the splitting of order in the proportion as stated in the RFP at the discretion of Bank.
13. We certify that while submitting our Bid document, we have not made any changes in the contents of the RFP document, read with its amendments/clarifications provided by the Bank.
14. If our bid is accepted, we are to be jointly and severally responsible for the due performance of the contract.
15. We ensured that salary payments to resources deployed for Bank's Project is done through Transfer mode from bidder's Bank a/c directly to credit into their specific salary accounts only. No cash payments are to be made to provide remuneration for services provided to the Bank on behalf of the selected bidder.
16. Bidder means the vendor(s) who is decided and declared so after examination of commercial bids.

17. We ensure that the entire data relating to payment systems operated by them will be stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction.
18. We confirm that Payment of statutory dues like PF, ESIC etc. are being made on time to the employees.

Date:

Place:

Bidder's Authorized Signatory

Designation

Bidder's name

Company Name and Seal

15.3 Annexure 3: Tender Covering Letter

Tender Covering Letter

(Should be submitted on Company's letter head)

General Manager
Punjab & Sind Bank
Second Floor
IT Department
Plot Number 151, Sector 44,
Gurugram, 122003

Dear Sir,

Sub: Selection of Bidder for Supply Installation, Implementation, Maintenance & Management of

Ref No. _____ dated _____

With reference to the above RFP, having examined and understood the instructions including all annexure, terms and conditions forming part of the Bid, we hereby enclose our offer for IT Service and Operation Management Solution in the RFP document forming Technical Bid as well as Commercial Bid being parts of the above referred Bid. I am authorized to sign the documents in this regard and the copy of authorization letter/ POA / Board resolution is attached herewith.

We agree to abide by and fulfil all the terms and conditions of the tender and in default thereof, to forfeit and pay to you or your successors, or authorized nominees such sums of money as are stipulated in the conditions contained in tender together with the return acceptance of the contract.

We confirm that we have noted the contents of the RFP and have ensured that there is no deviation in filing our response to the RFP and that the Bank will have the right to disqualify us in case of any such deviations.

Until a formal contract is executed, this tender offer, together with the Bank's written acceptance thereof and Bank's notification of award, shall constitute a binding contract between us. We understand that The Bank is not bound to accept the lowest or any offer the Bank may receive. We also certify that we have not been blacklisted by any PSU Bank/IBA/RBI at the time of Bid submission and at the time of bid submission.

All the details mentioned by us are true and correct and if the Bank observes any misrepresentation of facts on any matter at any stage, Bank has the absolute right to reject the proposal and disqualify us from the selection process. The bank reserves the right to verify /evaluate the claims made by the Bidder independently.

Dated this ____ day of _____, 2026

Authorized Signatory

Designation

Bidder's name

(Name of Address Authorized Signatory)

Company Name and Seal

15.4 Annexure 4: Bid Security Declaration

Bid Security Declaration

(To be stamped in accordance with stamp act)

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

Date: _____

To,

General Manager
Punjab & Sind Bank
Second Floor
IT Department
Plot Number 151, Sector 44,
Gurugram, 122003

Dear Sir,

We, the undersigned, declare that:

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

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

- Fails to honor submitted bid; and/or
- If the bidder withdraws the bid during the period of bid validity (180 days from the date of opening of bid).
- If the bidder makes any statement or encloses any form which turns out to be false, incorrect and / or misleading at any time prior to signing of contract and/or conceals or suppresses material information; and / or
- The selected bidder withdraws his tender before furnishing the unconditional and irrevocable Performance Bank Guarantee.
- The bidder violates any of the provisions of the terms and conditions of this tender specification.
- In case of the successful bidder, if the bidder fails:
 - To sign the contract in the form and manner to the satisfaction of Punjab & Sind Bank
 - To furnish Performance Bank Guarantee in the form and manner to the satisfaction of Punjab & Sind Bank either at the time of or before the execution of Agreement.
 - Bank may proceed against the selected bidder in the event of any evasion, avoidance, refusal or delay on the part of bidder to sign and execute the Purchase Order / Service Level Agreements or any other documents, as may be required by the Bank, if the bid is accepted.

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

Name of Signatory

Designation

15.5 Annexure 5: Pre-Qualification Criteria

Ref: RFP No. _____ dated _____

Eligibility criteria to be met mandatorily by the bidders:

#	Eligibility Criteria/Clause	Supporting Documents
1	Proof of Earnest Money Deposit	To be submitted along with the bid.
2	The Bidder should be operating in India as a registered company under Companies Act, 2013/1956 or LLP (Limited Liability Partnership) Act 2008 or Partnership firms registered under the Indian Partnership Act, 1932 with registered offices in India, and should be in existence in India for at least the last 5 (five) years as on date of opening of the bid	• Copy of Certificate of Incorporation or Partnership Deed • Copy of Registration Certificate/GST Registration certificate Copies of all documents listed above should be attested by authorized signatory and must be submitted along with the response.
3	The bidder should have valid PAN and GST Registration in India	Copy of Valid PAN Card and GST Registration Certificates issued by competent authority in India
4	The bidder should have a minimum average annual turnover of INR 1000 crore in India during the last 3 financial years (i.e. 2022-23, 2023-24 & 2024-25) along with positive net worth.	• CA Certificate* mentioning the turnover and net worth for each financial year and • Financial statements Audited (Balance sheet & Profit & Loss statement). The *CA certificate provided in this regard should be without any riders or qualification.
5	The bidder should be an authorized representative/ partner/ reseller of each of the proposed OEMs in India. MAF should be submitted from the following solution OEMs: 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. SSL Orchestrator along with packet broker 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network	MAF from the respective OEMs of the solution & services containing- 4. Name and address of the OEM and the name and address of the authorised bidder/entity. 5. Confirmation that the OEM shall honour and extend warranty and support for the products and services supplied by the authorised bidder/entity.

#	Eligibility Criteria/Clause	Supporting Documents
	6. Zero Trust Network Access (ZTNA) 7. Data Loss Prevention (DLP) 8. Information/Digital Right Management 9. Database Activity Monitoring 10. Mobile SDK 11. Host IPS including Application Change Control (HIPS) 12. Web Application Firewall (WAF) 13. Centralized key management solution 14. Certificate Lifecycle management 15. Identity & Access Management Solution 16. Multi Factor Authentication 17. Privilege Identity/Access Management 18. DNS Security Services (Internet-Facing DNS Security Services) 19. Cloud Access Security broker (CASB) 20. AI Security 21. SBOM/CBOM/AIBOM/QBOM	6. Confirmation that the bidder/entity is duly authorised by the OEM for supply, installation, implementation, technical support, maintenance and related services for the proposed solution(s). The MAF shall be submitted on the official letterhead of the respective OEM and must be signed by an authorised signatory having the authority to bind the OEM.”
6	Bidder must have at least enrolled manpower (on bidder’s payroll) of 150 experienced employees skilled in areas of Cyber/IT security.	Self-certification from the bidder
7	Bidder should have supplied, installed and maintained (or under maintenance) at least 10 of the below solutions in any one PSU/PSE/ BFSI/Government Organizations/ Regulatory & Statutory body in India: 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. SSL Interception/SSL offloader 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network/Anti-APT 6. Zero Trust Network Access (ZTNA)/Remote Access VPN 7. Data Loss Prevention (DLP)	Copy of Purchase Order/Work Order/ Contract AND In addition to the above, bidder to provide the following: d) Client credential/reference letter specifying the product deployed and the current status/stage of the project; OR e) Email confirmation from the client specifying the product deployed and the current status/stage of the project; OR

#	Eligibility Criteria/Clause	Supporting Documents
	8. Information/Digital Right Management 9. Database Activity Monitoring 10. Mobile SDK 11. Host IPS including Application Change Control (HIPS) 12. Web Application Firewall (WAF) (Mandatory Requirement) 13. Centralized key management solution 14. Certificate Lifecycle management 15. Identity & Access Management Solution 16. Multi Factor Authentication/2FA 17. Privilege Identity/Access Management 18. DNS Security Services (Internet-Facing DNS Security Services) Note: - c. Experience of solutions can be shown in single /multiple Clients/ work orders meeting the above criteria d. A bidder's experience in supplying and installing a solution will be considered regardless of when the installation was completed. Even if the installation was completed more than five years ago, it will still qualify, provided the bidder is currently maintaining that solution or has carried out its maintenance at any time during the five-year period preceding the RFP publication date.	f) Client-signed implementation signoff/ report confirming successful implementation of the solution; Note: The submitted documentary evidence must clearly identify the customer, the product/solution deployed, and the implementation and/or maintenance status relevant to the criterion for each of the products.
8	Bidder must have back-to-back support relation with all the proposed OEMs of solutions & services.	Self-Declaration from the bidder's authorized signatory stating the following: "We M/s _____ confirm that we shall backline with the respective solutions & services OEMs proposed through this RFP within 1 month of issuance of the Purchase order.

#	Eligibility Criteria/Clause	Supporting Documents
		We shall submit the relevant copy of the backlining agreement/ excerpt of the agreement/OEM confirmation for the duration of the contract” to substantiate the said clause.
9	If the bidder or its subsidiary or its associate or sister company or its holding company has already had an association with Punjab & Sind Bank in the past 5 years or at present as a service provider on any project, then the bidder is required to submit the satisfactory certificate from the bank issued/dated post the issuance of the RFP. Additionally, the Bidder should not have any Service Level Agreement/Contract pending to be signed with the Bank pending for more than 6 months from the date of issue of purchase order	Self-Certification from the bidder along with the satisfactory certificate from PSB (In case of association)
10	The Bidder to provide information that none of its subsidiaries or sister company or associate or holding company or companies having common director/s or companies in the same group of promoters/management or partnership firms/LLPs having common partners is not owned by any Director or Employee of the Bank.	Self-Certification from the bidder
11	The bidder shall submit a self-declaration confirming that, during the last three (3) years preceding the date of publication of this RFP, no contract, Purchase Order, or award issued by Punjab & Sind Bank (PSB) to the bidder has been cancelled, terminated, rescinded, or revoked due to non-performance, breach of obligations, or failure to comply with post-award requirements.	Self-Certification from the bidder
12	The Bidder should not have been blacklisted/ debarred by the Regulator / statutory body/ Government / Government agency / Banks / Financial Institutions in India during last 3 years and as on the date of bid submission.	Self-Certification from the bidder as per Annexure 11
13	The bidder should not be involved in any litigation which threatens the solvency of company.	Self-Certification from the bidder as per Annexure 10
14	Labor Law Compliance	Self-Certification from the bidder
15	Integrity Pact	Document on 100 Rs Stamp paper, duly signed and stamped by the authorized signatory.

#	Eligibility Criteria/Clause	Supporting Documents
16	Non-Disclosure Agreement	Document on 100 Rs Stamp paper, duly signed and stamped by the authorized signatory.
17	To avoid conflict of interest the successful bidder or its subsidiary or its associate or sister company or its holding company should not be the nextGEN SOC /SOC vendor of the bank under the existing	Self-declaration signed by Authorized Signatory of the bidder.
OEM Evaluation Criteria		
18	The proposed OEM solution/product should have been successfully implemented in least two Scheduled bank (including financial regulators). The reference implementation need not be of the same model, version, or product family as the proposed solution. List of Product which is required to comply with the above clause 18. Anti-Distributed Denial of Services (Anti-DDoS) 19. SSL Orchestrator along with packet broker 20. DNS protection (Internal DNS Security) 21. Web Gateway 22. Zero-Day Attack Protection at Endpoint and network 23. Zero Trust Network Access (ZTNA) 24. Data Loss Prevention (DLP) 25. Information/Digital Right Management 26. Mobile SDK 27. Host IPS including Application Change Control (HIPS) 28. Web Application Firewall (WAF) 29. Centralized key management solution 30. Certificate Lifecycle management 31. Database Access Management (DAM) 32. Identity & Access Management Solution 33. Multi Factor Authentication	Copy of Purchase Order/Work Order/ Contract In addition to the above, bidder to provide the following: “A client credential letter or email from the customer confirming the product used and the current stage of the project OR A client-signed implementation report or official sign-off confirming the work OR Self-Declaration from OEM confirming the product & stage of the project and reference to the PO”

#	Eligibility Criteria/Clause	Supporting Documents
	34. DNS Security Services (Internet-Facing DNS Security Services) Note: Experience should be during the five-year period preceding the RFP publication date. Even if the installation was completed more than five years ago, it will still qualify, provided the product is currently under maintenance or has been maintained at any time during the five-year period preceding the RFP publication date	
19	The proposed OEM solution/product for Privilege Identity/Access Management should have been successfully implemented in at least 2 BFSI in India, out of which at least one (1) BFSI Client should have a deployment covering more than 1,500 privileged users Note: Experience should be during the five-year period preceding the RFP publication date. Even if the installation was completed more than five years ago, it will still qualify, provided the product is currently under maintenance or has been maintained at any time during the five-year period preceding the RFP publication date	Copy of Purchase Order/Work Order/ Contract In addition to the above, bidder to provide the following: “A client credential letter or email from the customer confirming the product used and the current stage of the project OR A client-signed implemented report or official sign-off confirming the work OR Self-Declaration from OEM confirming the product & stage of the project and reference to the PO”
20	The proposed OEM solution/product should have been successfully implemented in at least 2 verifiable clients in India. The reference implementation need not be of the same model, version, or product family as the proposed solution. List of Product which is required to comply with the above clause	Copy of Purchase Order/Work Order/ Contract In addition to the above, bidder to provide the following: “A client credential letter or email from the customer confirming the product used and the current stage of the project

#	Eligibility Criteria/Clause	Supporting Documents
	4. AI Security 5. SBOM/CBOM/AIBOM/QBOM 6. Cloud Access Security broker (CASB) with minimum 100 Licenses each Note: Experience should be during the five-year period preceding the RFP publication date. Even if the installation was completed more than five years ago, it will still qualify, provided the product is currently under maintenance or has been maintained at any time during the five-year period preceding the RFP publication date	OR A client-signed implementation report or official sign-off confirming the work OR Self-Declaration from OEM confirming the product & stage of the project and reference to the PO”
21	Compliance with the FRS, TRS, SoW, SBOM & CBOM Solution List: 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. SSL Orchestrator along with packet broker 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network/Anti-APT 6. Zero Trust Network Access (ZTNA) 7. Data Loss Prevention (DLP) 8. Information/Digital Right Management 9. Database Activity Monitoring 10. Mobile SDK 11. Host IPS including Application Change Control (HIPS) 12. Web Application Firewall (WAF) 13. Centralized key management solution 14. Certificate Lifecycle management 15. Identity & Access Management Solution 16. Multi Factor Authentication 17. Privilege Identity/Access Management 18. DNS Security Services (Internet-Facing DNS Security Services) 19. Cloud Access Security broker (CASB)	Self-declaration, in the format Annexure 18, from the respective OEM for each of the products & services proposed on their letterhead signed by the authorized signatory

#	Eligibility Criteria/Clause	Supporting Documents
	20. AI Security 21. SBOM, CBOM, AIBOM & QBOM	
22	Functional Compliance: The Bidder's proposed solution shall be evaluated for functional compliance against the requirements specified in Appendix 1A: Functional Compliance Sheet. The proposed product should have minimum functional compliance score of 85% for each of the following: 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. SSL Orchestrator along with packet broker 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network 6. Zero Trust Network Access (ZTNA) 7. Data Loss Prevention (DLP) 8. Information/Digital Right Management 9. Database Activity Monitoring 10. Mobile SDK 11. Host IPS including Application Change Control (HIPS) 12. Web Application Firewall (WAF) 13. Centralized key management solution 14. Certificate Lifecycle management 15. Identity & Access Management Solution 16. Multi Factor Authentication 17. Privilege Identity/Access Management 18. DNS Security Services (Internet-Facing DNS Security Services) 19. Cloud Access Security broker (CASB) 20. AI Security	d) OEM Self Declaration e) Filled Appendix 1A: Functional Compliance f) Supporting Documentation like datasheets, product manuals, OEM website product feature listings etc.

#	Eligibility Criteria/Clause	Supporting Documents									
	21. SBOM, CBOM, AIBOM & QBOM Each product/solution shall be evaluated independently, and the compliance score shall be computed separately for each product/solution. <table> <tr> <th>Maximum Marks</th><th>Compliance (S/C)</th><th>Maximum Mark</th></tr> <tr> <td>10</td><td>S (Standard):</td><td>This indicates that the requirement is covered by the standard product functionality. It includes features available out-of-the-box, as well as those achievable through parametrization or rules configuration.</td></tr> <tr> <td>3</td><td>C (Customization):</td><td> Requirements marked as "C" are the ones that require minor modifications to the proposed solution. - Such customizations may include development of custom code, creation of new interfaces, user interface enhancements, or custom-built screens integrated with the base product. - All identified customizations shall be completed, tested, and made available by the bidder prior to commencement of User Acceptance Testing (UAT) (i.e, within 17 weeks of acceptance of </td></tr> </table>	Maximum Marks	Compliance (S/C)	Maximum Mark	10	S (Standard):	This indicates that the requirement is covered by the standard product functionality. It includes features available out-of-the-box, as well as those achievable through parametrization or rules configuration.	3	C (Customization):	Requirements marked as "C" are the ones that require minor modifications to the proposed solution. - Such customizations may include development of custom code, creation of new interfaces, user interface enhancements, or custom-built screens integrated with the base product. - All identified customizations shall be completed, tested, and made available by the bidder prior to commencement of User Acceptance Testing (UAT) (i.e, within 17 weeks of acceptance of	
Maximum Marks	Compliance (S/C)	Maximum Mark									
10	S (Standard):	This indicates that the requirement is covered by the standard product functionality. It includes features available out-of-the-box, as well as those achievable through parametrization or rules configuration.									
3	C (Customization):	Requirements marked as "C" are the ones that require minor modifications to the proposed solution. - Such customizations may include development of custom code, creation of new interfaces, user interface enhancements, or custom-built screens integrated with the base product. - All identified customizations shall be completed, tested, and made available by the bidder prior to commencement of User Acceptance Testing (UAT) (i.e, within 17 weeks of acceptance of									

#	Eligibility Criteria/Clause			Supporting Documents
			PO), without impacting the Bank's project timelines. 6. Only those changes that can be implemented without altering the base product and without impacting future upgrades, patches, or vendor support shall qualify as Customization (C)	

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

- Attested copies of all relevant documents, certificates, work orders, completion certificates, financial statements, and other supporting documents shall be submitted as documentary evidence in support of the claims made by the bidder. The bidder shall furnish any additional information and clarification as may be required by the Bank for verification of eligibility criteria. The Bank reserves the right to independently verify, evaluate, and validate the information and claims submitted by the bidder. The decision of the Bank in this regard shall be final, conclusive, and binding on the bidder.
- In the event of a business transfer, acquisition, slump sale, merger, or acquisition of a business undertaking, the work experience, credentials, and references of the transferor entity ("Seller") pertaining to the acquired business may be considered, subject to submission of documentary evidence establishing such transfer and continuity of business operations.
- In cases involving corporate restructuring, including merger, amalgamation, demerger, name change, conversion, or reorganization, the incorporation certificate, financial statements, work experience credentials, technical qualifications, and other relevant records of the predecessor entity may be considered, subject to submission of documentary evidence acceptable to the Bank.
- Either the Principal/OEM or its authorized agent may submit a bid for a given item/product under this RFP. However, both the Principal/OEM and its authorized agent shall not be permitted to submit bids simultaneously for the same item/product in the same RFP. Further, where an agent is authorized to represent a Principal/OEM, the same agent shall not submit bids on behalf of more than one Principal/OEM for the same item/product under this RFP. Any violation of the above conditions shall render all such bids liable for rejection at the sole discretion of the Bank.

- e. The bidder and/or OEM shall comply with applicable guidelines issued by the Central Vigilance Commission (CVC), including Circular No. 03/01/12, the applicable provisions of the General Financial Rules (GFR), and the Department of Expenditure Office Memorandum dated 25.07.2016, as amended from time to time.
- f. In a tender, either the Indian Agent on behalf of the Principal/OEM or the Principal/OEM itself may bid; however, both shall not bid simultaneously for the same item/product in the same tender.
- g. Documentary evidence shall be furnished against each eligibility criterion along with a detailed index of documents submitted. All documents shall be duly signed and stamped by the Authorized Signatory of the bidder. Relevant sections of the submitted documents supporting compliance with the eligibility criteria shall be clearly highlighted for ease of verification by the Bank.
- h. Any misrepresentation, suppression of facts, submission of forged/fabricated documents, or provision of incorrect information by the bidder at any stage of the bidding process may result in rejection of the bid, forfeiture of bid security (if applicable), and/or blacklisting/debarment from participating in future procurement processes of the Bank, without prejudice to any other rights and remedies available to the Bank under law.
- i. For the purpose of this RFP, the term "Scheduled Bank" shall exclude Regional Rural Banks (RRBs) and Payment banks. Accordingly, experience shall be considered for the purpose of evaluating eligibility and qualification criteria under this RFP.
- j. Deployments shall be considered valid only if the solution has been used for its intended function in a production environment. Tests, pilot, or non-production deployments shall not be accepted.
- k. Experience of solution(s) can be shown in single /multiple Clients/work orders meeting the criteria(s)
- l. Experience should be during the five-year period preceding the RFP publication date. Even if the installation was completed more than five years ago, it will still qualify, provided the product is currently under maintenance or has been maintained at any time during the five-year period preceding the RFP publication date
- m. Experience must be showcased separately for each solution category, with clear evidence that each solution has been deployed as a standalone solution and not merely as a feature or component of another solution.
- n. When deemed necessary the Evaluation Committee may seek clarification on relevant aspects from the Bidder. However, that would not entitle the Bidder to change or cause any change.
- o. Bank reserves the right to conduct reference site visit/ video conference/ voice call with the Client to substantiate the credentials/ copy of PO/ Contract copy/ sign-off submitted by Bidder and/ or OEM. In case the input/ feedback received from the Customer is negative/ unsatisfactory, bank reserves the right to reject the Bid



Selection of Bidder for Supply Installation,
Implementation, Maintenance & Management
of IT Security Solutions & Services

Date

Signature with seal

Name:

Designation:

15.6 Annexure 6: Acceptance/Compliance Certificate

ACCEPTANCE/ COMPLIANCE CERTIFICATE

Ref: RFP No. _____ dated _____

All Terms and Conditions including scope of work

We hereby undertake and agree to abide by all the terms and conditions, scope of work & other terms stipulated by the Bank in this RFP including all addendum, corrigendum, clarification issued by bank etc.

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

Any assumptions, deviation or exclusions may result in the disqualification of our bids.

We also understand that the bank may not consider our assumptions, deviations or exclusions quoted by us anywhere in the proposal during the evaluation or during the contract period and we shall be liable make necessary arrangements at no additional cost to the bank in order to meet the requirements stated in the RFP including all addendum, corrigendum, clarification issued by bank etc.

Signature:

Seal of company

15.7 Annexure 7: Minimum Local Content Certification

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

TENDER REREFERENCE NUMBER: _____

Date:

To,

General Manager
Punjab & Sind Bank
Second Floor
IT Department
Plot Number 151, Sector 44,
Gurugram, 122003

Dear Sir,

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

Signature of Authorized Signatory

Name:

Date:

Designation:

Seal:

15.8 Annexure 8: Certification on OEM Requirements

RFP No:

(Letter to be submitted by the OEM's letter head)

To,
General Manager
Punjab & Sind Bank
Second Floor
IT Department
Plot Number 151, Sector 44,
Gurugram, 122003

Dear Sir,

Sub: Request for proposal Selection of Bidder for Supply Installation, Implementation, Maintenance & Management of _____ vide RFP No: _____

We, who are established and reputable manufacturers / producers of _____ having factories / development facilities at _____ (address of factory / facility) confirms the following:

- i. Scope of work pertaining to Requirement analysis, System design, Development & implementation, Documentation, Final Deployment and Go-live will be performed by us for our proposed product as mentioned in the RFP.
- ii. We will provide our highest-level support during the O&M, warranty, ATS & AMC phase
- iii. We also confirm that, starting from Year 2 and continuing annually during the Operations and Management phase, our personnel will conduct a comprehensive review of configurations, rules, and parameterizations, as well as a solution architecture review for all PSB environments related to our product. This review will also address any observations raised by regulators concerning the implementation of our solution in the Bank. A detailed report of the review will be submitted directly to the designated SPOC at PSB by our assigned project manager.
- iv. Additionally, we will liaison with the bidder to close all the observation in the review report, if required, or we shall close through our personnel. Timelines to close the issue would be discussed and agreed with the bank while submitting the report based on the criticality defined in the report, based on the discussion.

Yours faithfully
Authorized Signatory
(Name of manufacturers):

Place:

Name:

Date:

Phone No.:

Fax:

E-mail:

15.9 Annexure 9: Escalation Matrix

Escalation Matrix

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

Ref: RFP No. _____ dated _____.

Name of the Company/Firm:

Service-Related Issues

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

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

Date

Signature with seal

Name:

Designation:

15.10 Annexure 10: Litigation Certificate

Litigation Certificate

Reg.: Selection of Bidder for Supply Installation, Implementation, Maintenance & Management of

To be provided by Statutory Auditor/Chartered Accountant

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

Date: _____

Place: _____

Signature of CA/Statutory Auditor

Name of CA/Statutory Auditor:

Designation:

Email ID:

Mobile No:

Telephone No.:

Seal of Company:

15.11 Annexure 11: Non-blacklisting undertaking

Undertaking for non-blacklisting

To,

General Manager
Punjab & Sind Bank
Second Floor
IT Department
Plot Number 151, Sector 44,
Gurugram, 122003

Dear Sir,

Reg.: Selection of Bidder for Supply Installation, Implementation, Maintenance & Management of _____

We M/s _____, a company incorporated under the companies act, 1956 with its headquarters at, _____ do hereby confirm that we have not been blacklisted/ debarred by the Regulator / statutory body/ Government / Government agency / Banks / Financial Institutions in India during last 3 years and as on the date of bid submission.

This declaration has been submitted and limited to, in response to the tender reference mentioned in this document

Thanking You,

Yours faithfully,

Date: _____

Place: _____

Signature of Authorized Signatory

Name of Signatory:

Designation:

Email ID:

Mobile No:

Telephone No.:

Seal of Company:

15.12 Annexure 12: Undertaking of Authenticity (on bidder's letterhead)

To:

(Name and address of Procuring Office)

Sub: Undertaking of Authenticity for supplied Product(s)

Ref: RFP No. _____ dated _____

With reference to the Product being quoted to you vide our Bid No: _____ dated _____, we hereby undertake that all the components /parts /assembly / software etc. used in the Product to be supplied shall be original new components / parts / assembly / software only, from respective Original Equipment Manufacturers (OEMs) of the Products and that no refurbished / duplicate / second hand components /parts/ assembly / software shall be supplied or shall be used or no malicious code are built-in in the Product being supplied.

1. We also undertake that in respect of licensed operating systems and other software utilities to be supplied, the same will be sourced from authorized sources and supplied with Authorized License Certificate (i.e. Product keys on Certification of Authenticity in case of Microsoft Windows Operating System).
2. Should you require, we hereby undertake to produce the certificate from our OEM supplier in support of above undertaking at the time of delivery/installation. It will be our responsibility to produce such letters from our OEM supplier's at the time of delivery or within a reasonable time.
3. In case of default and/or the Bank finds that the above conditions are not complied with, we agree to take back the Product(s) supplied and return the money paid by you, in full within seven days of intimation of the same by the Bank, without demur or any reference to a third party and without prejudice to any remedies the Bank may deem fit.
4. We also take full responsibility of both Product(s) & Service(s) as per the content of the RFP even if there is any defect by our authorized Service Centre / Reseller / SI etc.

Dated this day of 2026

(Signature)

(Name)

(In the capacity of)

Duly authorised to sign Bid for and on behalf of _____

15.13 Annexure 13: Non-Disclosure Agreement

NON-DISCLOSURE AGREEMENT

All bidders must sign the Non-Disclosure Agreement (NDA) while submitting the response to the Request for proposal (RFP). Bidders must comply with all clauses mentioned in the NDA. No changes to the NDA are allowed.

NDA format is provided below.

(To be stamped in accordance with stamp act)

Strictly Private and Confidential

This Non-Disclosure Agreement made and entered into at..... Thisday.....of.....20.....BY AND BETWEEN , a company incorporated under the Companies Act, 1956 having its registered office at (Hereinafter referred to as the Bidder which expression unless repugnant to the context or meaning thereof be deemed to include its permitted successors) of the ONE PART;

AND

Punjab & Sind Bank, a body corporate, established under the Banking Companies (Acquisition and Transfer of Undertakings) Act 1980 and having its (hereinafter referred to as "Bank" which expression shall unless it be repugnant to the subject, meaning or context thereof, be deemed to mean and include its successors and assigns) of the OTHER PART.

The Bidder and Punjab & Sind Bank are hereinafter collectively referred to as "the Parties" and individually as "the Party".

WHEREAS:

1. Punjab & Sind Bank is engaged in the business of providing financial services to its customers and intends to engage service provider _____
2. In the course of such an assignment, it is anticipated that Punjab & Sind Bank or any of its officers, employees, officials, representatives or agents may disclose, or deliver, to the Bidder some Confidential Information (as hereinafter defined), to enable the Bidder to carry out the aforesaid Implementation assignment (hereinafter referred to as " the Purpose").
3. The Bidder is aware and confirms that all information, data and other documents made available in the RFP/Bid Documents/Agreement /Contract or in connection with the Services

rendered by the Bidder are confidential information and are privileged and strictly confidential and or proprietary of Punjab & Sind Bank. The Bidder undertakes to safeguard and protect such confidential information as may be received from Punjab & Sind Bank.

NOW, THEREFORE THIS AGREEMENT WITNESSED THAT in consideration of the above premises and the Punjab & Sind Bank granting the Bidder and or his agents, representatives to have specific access to Punjab & Sind Bank property / information and other data it is hereby agreed by and between the parties hereto as follows:

4. Confidential Information:

- (i) "Confidential Information" means all information disclosed/furnished by Punjab & Sind Bank to the Bidder whether orally, in writing or in electronic, magnetic or other form for the limited purpose of enabling the Bidder to carry out the proposed Implementation assignment, and shall mean and include data, documents and information or any copy, abstract, extract, sample, note or module thereof, explicitly designated as "Confidential"; Provided the oral information is set forth in writing and marked "Confidential" within seven (7) days of such oral disclosure.
- (ii) The Bidder may use the Confidential Information solely for and in connection with the Purpose and shall not use the Confidential Information or any part thereof for any reason other than the Purpose stated above.

Confidential Information in oral form must be identified as confidential at the time of disclosure and confirmed as such in writing within seven (7) days of such disclosure. Confidential Information does not include information which:

- (a) is or subsequently becomes legally and publicly available without breach of this Agreement by either party,
- (b) was rightfully in the possession of the Bidder without any obligation of confidentiality prior to receiving it from Punjab & Sind Bank,
- (c) was rightfully obtained by the Bidder from a source other than Punjab & Sind Bank without any obligation of confidentiality,
- (d) was developed by for the Bidder independently and without reference to any Confidential Information and such independent development can be shown by documentary evidence, or is/was disclosed pursuant to an order of a court or governmental agency as so required by such order, provided that the Bidder shall, unless prohibited by law or regulation, promptly notify Punjab & Sind Bank of such order and afford Punjab & Sind Bank the opportunity to seek appropriate protective order relating to such disclosure.
- (e) the recipient knew or had in its possession, prior to disclosure, without limitation on its confidentiality.
- (f) is released from confidentiality with the prior written consent of the other party.

The recipient shall have the burden of proving hereinabove are applicable to the information in the possession of the recipient. Confidential Information shall at all times remain the sole and exclusive property of the disclosing party. Upon termination of this Agreement, Confidential Information shall be returned to the disclosing party or destroyed, if incapable of return. The destruction shall be witnessed and so recorded, in writing, by an authorized representative of each of the parties.

Nothing contained herein shall in any manner impair or affect the rights of Punjab & Sind Bank in respect of the Confidential Information.

In the event that any of the Parties hereto becomes legally compelled to disclose any Confidential Information, such Party shall give sufficient notice to the other party to enable the other Party to prevent or minimize to the extent possible, such disclosure. Neither party shall disclose to a third party any Confidential Information or the contents of this Agreement without the prior written consent of the other party. The obligations of this Clause shall be satisfied by handling Confidential Information with the same degree of care, which the receiving party applies to its own similar confidential information but in no event less than reasonable care.

The obligations of this clause shall survive the expiration, cancellation, or termination of this Agreement and for a period of five (5) years with respect to project confidentiality. However, confidentiality obligations with respect to individually identifiable information, data/ information classified as PII, any customer's data of bank and any IPR of the bank shall survive in perpetuity.

5. N
on-disclosure: The Bidder shall not commercially use or disclose any Confidential Information, or any materials derived there from to any other person or entity other than persons in the direct employment of the Bidder who have a need to have access to and knowledge of the Confidential Information solely for the Purpose authorized above. The Bidder shall take appropriate measures by instruction and written agreement prior to disclosure to such employees to assure against unauthorized use or disclosure. The Bidder may disclose Confidential Information to others only if the Bidder has executed a Non-Disclosure Agreement with the other party to whom it is disclosed that contains terms and conditions that are no less restrictive than these presents, and the Bidder agrees to notify Punjab & Sind Bank immediately if it learns of any use or disclosure of the Confidential Information in violation of terms of this Agreement.

Notwithstanding the marking and identification requirements above, the following categories of information shall be treated as Confidential Information under this Agreement irrespective of whether it is marked or identified as confidential:

- a) Information regarding Punjab & Sind Bank and any of its Affiliates, customers and their accounts ("Customer Information"). For purposes of this Agreement, Affiliate means a business entity now or hereafter controlled by, controlling or under common control. Control exists when an entity owns or controls more than 10% of the outstanding shares or securities representing the right to vote for the election of directors or other managing authority of another entity; or
- b) any aspect of Punjab & Sind Bank's business that is protected by patent, copyright, trademark, trade secret or other similar intellectual property right; or
- c) business processes and procedures; or
- d) current and future business plans; or
- e) personnel information; or
- f) Financial information.

6. **Publications:** The Bidder shall not make news releases, public announcements, give interviews, issue or publish advertisements or publicize in any other manner whatsoever in connection with this Agreement, the contents / provisions thereof, other information relating to this Agreement, the Purpose, the Confidential Information or other matter of this Agreement, without the prior written approval of Punjab & Sind Bank. sss

7. **Term:** This Agreement shall be effective from the date hereof and shall continue till expiration of the Purpose or termination of this Agreement by Punjab & Sind Bank, whichever is

earlier. The Bidder hereby agrees and undertakes to Punjab & Sind Bank that immediately on termination of this Agreement it would forthwith cease using the Confidential Information and further promptly return or destroy, under information to Punjab & Sind Bank, all information received by it from Punjab & Sind Bank for the Purpose, whether marked Confidential or otherwise, and whether in written, graphic or other tangible form and all copies, abstracts, extracts, samples, notes or modules thereof. The Bidder further agree and undertake to Punjab & Sind Bank to certify in writing upon request of Punjab & Sind Bank that the obligations set forth in this Agreement have been complied with.

Any provisions of this Agreement which by their nature extend beyond its termination shall continue to be binding and applicable without limit in point in time except and until such information enters the public domain

8. T
Title and Proprietary Rights: Notwithstanding the disclosure of any Confidential Information by Punjab & Sind Bank to the Bidder, the title and all intellectual property and proprietary rights in the Confidential Information shall remain with Punjab & Sind Bank.

9. R
Remedies: The Bidder acknowledges the confidential nature of Confidential Information and that damage could result to Punjab & Sind Bank if the Bidder breaches any provision of this Agreement and agrees that, if it or any of its directors, officers or employees should engage or cause or permit any other person to engage in any act in violation of any provision hereof, Punjab & Sind Bank may suffer immediate irreparable loss for which monetary compensation may not be adequate. Punjab & Sind Bank shall be entitled, in addition to other remedies for damages & relief as may be available to it, to an injunction or similar relief prohibiting the

Bidder, its directors, officers etc. from engaging in any such act which constitutes or results in breach of any of the covenants of this Agreement.

Any claim for relief to Punjab & Sind Bank shall include Punjab & Sind Bank's costs and expenses of enforcement (including the attorney's fees).

10. E
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.

11. D
Dispute Resolution: If any dispute, difference or claim arises between the parties hereto in connection with the validity, interpretation, implementation or alleged breach of the terms of this Agreement or anything done or omitted to be done pursuant to this Agreement, the Parties shall attempt in the first instance to resolve the same through negotiation. If the dispute is not resolved through negotiation within 30 (thirty) days after commencement of discussions, then, the parties shall be at liberty to approach competent court of law at Delhi for adjudication of the disputes.

12. G
Governing Law: Governing Law: The laws of India shall govern this Agreement

13. J
Jurisdiction: It is hereby agreed between the parties that any suit or legal proceedings to enforce

the rights of either party under this Agreement shall be instituted and tried by a competent court in the city of Delhi only.

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

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

- Natural phenomenon, including but not limited to floods, droughts, earthquakes, epidemics and pandemics
- Acts of any government, including but not limited to war, declared or undeclared priorities, quarantines and embargos
- Terrorist attack, public unrest in work area
- Provided either party shall within 10 days from occurrence of such a cause, notify the other in writing of such causes. The Bidder or The Bank shall not be liable for delay in performing his/her obligations resulting from any force Majeure cause as referred to and/or defined above. Any delay beyond 30 days shall lead to termination of contract by parties and all obligations expressed quantitatively shall be calculated as on date of termination. Notwithstanding this, provisions related to indemnity, confidentiality survive termination of the contract.
- Unless otherwise directed by the bank in writing, the Bidder affected by force majeure shall continue to perform the obligations under this agreement, which are not affected by the force majeure event and shall take such steps as are reasonably necessary to remove the causes resulting in force majeure and to mitigate the effect thereof.
- As soon as the cause of force majeure has been removed, the Bidder shall notify the Bank and resume the affected activity without delay.
- Notwithstanding the above, the decision of the bank shall be final and binding on the Bidder in the event of force majeure.

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

17. G
General: The Bidder shall not reverse - engineer, decompile, disassemble or otherwise interfere with any software disclosed hereunder.

18. A
All Confidential Information is provided “as is”. In no event shall the Punjab & Sind Bank be liable for the inaccuracy or incompleteness of the Confidential Information. None of the Confidential Information disclosed by Punjab & Sind Bank constitutes any representation, warranty, assurance, guarantee or inducement with respect to the fitness of such Confidential Information for any particular purpose.

19. P
Punjab & Sind Bank discloses the Confidential Information without any representation or warranty, whether express, implied or otherwise, on truthfulness, accuracy, completeness, lawfulness, merchant ability, fitness for a particular purpose, title, non-infringement, or anything else.

20. W
Waiver: A waiver (whether express or implied) by Punjab & Sind Bank of any of the provisions of this Agreement, or of any breach or default by the Bidder in performing any of the provisions hereof, shall not constitute a continuing waiver and such waiver shall not prevent Punjab & Sind Bank from subsequently enforcing any of the subsequent breach or default by the Bidder under any of the provisions of this Agreement.

In witness whereof, the Parties hereto have executed these presents the day, month and year first herein above written.

For and on behalf of _____	For and on behalf of Punjab & Sind Bank

15.14 Annexure 14: Commercial Proposal Submission Checklist

Instructions to be noted while preparing/submitting Part B - Commercial Proposal

All Annexure or appendix should be submitted in Bidder's Letter Head with seal and signature of the authorized signatory.

1. Bill of Material as per Appendix 2.

15.15 Annexure 15: Bank Guarantee Format for Earnest Money Deposit

Performa for the Bank Guarantee for Earnest Money Deposit

(To be stamped in accordance with stamp act)

Ref: Bank Guarantee #

Date: _____

To,

General Manager
Punjab & Sind Bank
Second Floor
IT Department
Plot Number 151, Sector 44,
Gurugram, 122003

Dear Sir,

In accordance with your bid reference No. _____ Dated _____ M/s _____ having its registered office at _____ herein after Called „bidder“) wish to participate in the said bid for Selection of Bidder(s) for Supply Installation, Implementation, Maintenance & Management of _____. An irrevocable Financial Bank Guarantee (issued by a nationalized /scheduled commercial Bank) against Earnest Money Deposit amounting to Rs. valid up to _____ is required to be submitted by the bidder, as a condition for participation in the said bid, which amount is liable to be forfeited on happening of any contingencies mentioned in the bid document. M/s _____ having its registered office at _____ has undertaken in pursuance of their offer to Punjab & Sind Bank (hereinafter called as the beneficiary) dated _____ has expressed its intention to participate in the said bid and in terms thereof has approached us and requested us _____ (Name of Bank) _____ (Address of Bank) to issue an irrevocable financial Bank Guarantee against Earnest Money Deposit (EMD) amounting to Rs _____ (Rupees _____) valid up to _____. We, the _____ (Name of Bank) _____ (Address of Bank) having our Head office at _____ therefore Guarantee and undertake to pay immediately on first written demand by Punjab & Sind, the amount Rs. _____ (Rupees _____) without any reservation, protest, demur and recourse in case the bidder fails to Comply with any condition of the bid or any violation against the terms of the bid, Without the beneficiary needing to prove or demonstrate reasons for its such demand. Any Such demand made by said beneficiary shall be conclusive and binding on us irrespective of any dispute or difference raised by the bidder. This guarantee shall be irrevocable and

shall remain valid up to _____. If any further extension of this Guarantee is required, the same shall be extended to such required period on receiving instructions in writing, from Punjab & Sind Bank, on whose behalf guarantee is issued. "Notwithstanding anything contained herein above Our liability under this bank guarantee shall not exceed Rs. _____ (Rupees _____).

This bank guarantee shall be valid up to _____. We are liable to pay the guaranteed amount or any part thereof under this bank guarantee only if you serve upon us a written claim or demand, on or before _____ before _____ hours (Indian Standard Time) or within Bank official working hours where after it ceases to be in effect in all respects whether or not the original bank guarantee is returned to us." In witness whereof the Bank, through its authorized officer has set its hand stamped on this _____ Day of _____ 2026 at _____

Name of signatory

Bank Common Seal

Designation

15.16 Annexure 16: Format of Performance Guarantee

(Issued by any Scheduled Commercial Bank & to be executed on stamp paper of requisite value as per stamp duty payable at place of execution.)

Tender Reference No: _____ Date _____

To,

General Manager
Punjab & Sind Bank
Second Floor
IT Department
Plot Number 151, Sector 44,
Gurugram, 122003

Dear Sir,

1. WHEREAS pursuant to a Request for Proposal dated..... (hereinafter referred to as RFP, issued by Punjab & Sind Bank, HEAD OFFICE IT DEPARTMENT , 2ND FLOOR,PLOT NO. 151, SECTOR 44 INSTITUTIONAL AREA, GURUGRAM -122003 in response of (Bidder(s) / Service Provider), a Company registered under the Companies Act, 1956 and having its Registered / Corporate Office athas awarded the Contract valued Rs.....and appointed.....as Bidder(s) / Service Provider for procurement of IT Service and Operation Management Solution vide Appointment letter / Purchase Order No.....dated.....on the terms and conditions as set out inter-alia in the said RFP and in the Appointment Letter / Purchase Order.
2. WHEREAS you have in terms of the said Appointment letter / Purchase Order called upon (Bidder(s) / Service Provider to furnish a Performance Guarantee, for Rs.....Rupees only), equivalent to.....of the Contract value, to be issued by a Bank in your favour towards due performance of the Contract in accordance with the specifications, terms and conditions of the said Appointment letter / Purchase Order and an Agreement entered / to be entered into in this behalf.
3. WHEREAS (Bidder(s) / Service Provider) has approached us for issuing in your favour a performance Guarantee for the sum of Rs.....(Rupees.....).

NOW THEREFORE in consideration of you having awarded the Contract to.....inter-alia on the terms & conditions that provides a performance guarantee for due performance of the terms and conditions thereof. We,.....Bank,..... a body corporate constituted underhaving its Head office at.....(give full address) and a branch inter-alia at..... India at the request of.....do hereby expressly, irrevocably and unconditionally undertake to pay merely on demand from you and without any demur without referring to any other source, Rs.....(Rupees.....only) against any loss or damage

caused to or suffered by or that may be caused to or suffered by you on account of any breach or breaches on the part ofof any of the terms and conditions of the Contract and in the event of.....committing any default or defaults in carrying out any of the work or discharging any obligation under the said Contract or otherwise in the observance and performance of any of the terms and conditions relating thereto including non-execution of the Agreement as may be claimed by you on account of breach on the part ofof their obligations or default in terms of the said Appointment letter / Purchase Order.

4. Notwithstanding anything to the contrary contained herein or elsewhere, we agree that your decision as to whether thehas committed any such breach / default or defaults and the amount or amounts to which you are entitled by reasons thereof will be binding on us and we shall not be entitled to ask you to establish its claim or claims under this Guarantee, but will pay the same forthwith on demand without any protest or demur. Any such demand made by you shall be conclusive as regards the amount due and payable by us to you.
5. This Guarantee shall be valid up to plus 12 months of the Claim period from the expiry of said guarantee period. Without prejudice to your claim or claims arisen and demanded from or otherwise notified to us in writing before the expiry of the said date which will be enforceable against us notwithstanding that the same is or are enforced after the said date.
6. You will have the fullest liberty without our consent and without affecting our liabilities under this Guarantee from time to time to vary any of the terms and conditions of the said appointment letter or the Contract to be made pursuant thereto or extend the time of performance of the Contract or to postpone for any time or from time to time any of your rights or powers against theand either to enforce or forbear to enforce any of the terms and conditions of the said appointment letter or the Contract and we shall not be released from our liability under Guarantee by exercise of your liberty with reference to matters aforesaid or by reason of any time being given to or any other forbearance, act or omission on your part or any indulgence by you or any other act, matter or things whatsoever which under law relating to sureties, would but for the provisions hereof have the effect of releasing us from our liability hereunder provided always that nothing herein contained will enlarge our liability hereunder beyond the limit of Rs..... (Rupees.....only) as aforesaid or extend the period of the guarantee beyond(date) unless expressly agreed to by us in writing.
7. This Guarantee shall not in any way be affected by you are taking or giving up any securities fromor any other person, firm or company on its behalf or by the winding up, dissolution, insolvency as the case may be of
8. In order to give full effect to the Guarantee herein contained, you shall be entitled to act as if we were your principal debtors in respect of all your claims againsthereby guaranteed by us as aforesaid and we hereby expressly waive all our rights of surety ship and other rights, if any, which are in any way inconsistent with any of the provisions of Guarantee.
9. Subject to the maximum limit of our liability as aforesaid, this Guarantee will cover all your claim or claims againstfrom time to time arising out of or in relation to the said appointment letter / Contract and in respect of which your claim in writing is lodged on us before expiry of Guarantee.
10. Any Notice by way of demand or otherwise hereunder may be sent by special courier, telex, fax, e-mail or registered post to our Head Office / Local address as aforesaid and if sent accordingly it shall be deemed to have been given when the same has been posted.
11. This Guarantee shall not be affected by any change in the constitution of _____ or nor shall it be affected by any change in your constitution or by any amalgamation or absorption thereof or

therewith but will ensure to the benefit of and be available to and be enforceable by the absorbing or amalgamated company or concern.

12. This Guarantee shall come into force from the date of its execution and shall not be revoked by us any time during its currency without your previous consent in writing.
13. We further agree and undertake to pay you the amount demanded in writing irrespective of any dispute or controversy between you and _____ in any suit or proceeding pending before any court, Tribunal or Arbitrator relating thereto, our liability under these presents being absolute and unequivocal. The payments so made by us shall be a valid discharge of our liability for payment hereunder and _____ shall have no claim against us for making such payment.
14. We have the power to issue this Bank Guarantee in your bank's favour as the undersigned has full power to execute this Bank Guarantee under the Power of Attorney issued by our Bank.
15. Our authority to issue this guarantee may be verified with our Controlling Office situated at _____ (full details of persons to be contacted address and phone Numbers etc).
16. Notwithstanding anything contained herein above;
 - i. Our liability under this Guarantee shall not exceed
Rs _____ (Rupees _____ only
)
 - ii. This Guarantee shall be valid and remain in force up to _____ plus the
Claim period of 12(Twelve) months and including the date _____
and
 - iii. We are liable to pay the guaranteed amount or any part thereof under this Guarantee only
and only if you serves upon us a written claim or demand for payment on or before the
expiry of this Guarantee. ss

Dated this the _____ day of _____ 2026

Signature and Seal of Guarantors

Bidder(s)'s Bank

15.17 Annexure 17 : Pre-contract integrity pact

(To be stamped in accordance with stamp act)

PRE-CONTRACT INTEGRITY PACT

Between

Punjab & Sind Bank (PSB) hereinafter referred to as "The Principal",

And

_____ hereinafter referred to as "The Bidder/ Contractor"

Preamble

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

In order to achieve these goals, the Principal has appointed

1. Sh. Debal Kumar Gayen (Gayen.dk@gmail.com) and
2. Sh. Pramod Kumar Garg (pkgarg.1957@gmail.com)

as Independent External Monitors (IEMs) who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

Section 1 - Commitments of the Principal

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

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

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

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

(2) If the Principal obtains information regarding the conduct of any of its employees which constitutes, or gives rise to reasonable suspicion of, an offence under the Bharatiya Nyaya Sanhita, 2023, the Prevention of Corruption Act, 1988, or any other applicable law, the Principal shall promptly inform the Chief Vigilance Officer and may initiate appropriate disciplinary action in accordance with applicable rules and regulations.

Section 2 - Commitments of the Bidder(s)/ Contractor(s)

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

a. The Bidder(s)/ Contractor(s) will not, directly or through any other person or firm, offer, promise or give to any of the Principal's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he / she is not legally entitled to, in order to obtain in exchange any advantage of 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 contract submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelisation in the bidding process.

c. The Bidder(s)/ Contractor(s) will not commit any offence under the relevant Bharatiya Nyaya Sanhita, 2023 Act; further the Bidder(s)/ Contractor(s) will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

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

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

f. Bidder(s) /Contractor(s) who have signed the Integrity Pact shall not approach the Courts while representing the matter to IEMs and shall wait for their decision in the matter.

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

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

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

Section 4 - Compensation for Damages

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

(2) If the Principal has terminated the contract according to Section 3, or if the Principal is entitled to terminate the contract according to Section 3, the Principal shall be entitled to demand and recover from the Contractor liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee.

Section 5 - Previous transgression

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

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

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

(1) In case of Sub-contracting, the Principal Contractor shall take the responsibility of the adoption of Integrity Pact by the Sub-contractor.

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

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

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

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

Section 8 - Independent External Monitor

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

(2) The Monitor is not subject to instructions by the representatives of the parties and performs his/her functions neutrally and independently. The Monitor would have access to all Contract documents, whenever required. It will be obligatory for him / her to treat the information and documents of the Bidders/Contractors as confidential. He/ she reports to the MD & CEO of Punjab & Sind Bank.

(3) The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the Principal including that provided by the Contractor. The Contractor will also grant the Monitor, upon his/her request and demonstration of a valid interest, unrestricted and unconditional access to their project documentation. The same is applicable to Sub-contractors.

(4) The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/ Contractor(s)/ Sub-contractor(s) with confidentiality. The Monitor has also signed declarations on 'Non-Disclosure of Confidential Information' and of 'Absence of Conflict of Interest'. In case of any conflict of interest arising at a later date, the IEM shall inform MD & CEO of Punjab & Sind Bank and recuse himself / herself from that case.

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

(6) As soon as the Monitor notices, or believes to notice, a violation of this agreement, he/she will so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.

(7) The Monitor will submit a written report to the MD & CEO of Punjab & Sind Bank, within 8 to 10 weeks from the date of reference or intimation to him by the Principal and, should the occasion arise, submit proposals for correcting problematic situations.

(8) If the Monitor has reported to the MD & CEO of Punjab & Sind Bank, a substantiated suspicion of an offence under relevant Bharatiya Nyaya Sanhita, 2023 Act, and the MD & CEO of Punjab & Sind Bank has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

(9) The word 'Monitor' would include both singular and plural

Section 9 - Pact Duration

This Pact begins when both parties have legally signed it. It expires for the Contractor 12 months after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded. Any violation of the same would entail disqualification of the bidders and exclusion from future business dealings.

If any claim is made / lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged / determined by MD & CEO of Punjab & Sind Bank.

Section 10 - Other provisions

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

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

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

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

(5) Issues like Warranty / Guarantee etc. shall be outside the purview of IEMs.

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

(For & On behalf of the Principal)
Contractor)

(For & On behalf of Bidder /

Place -----

Date -----

Witness 1:

(Name & Address)

Witness 2:
(Name & Address)

15.18 Annexure 18: Compliance with FRS, TRS, SoW & SBOM (on respective OEM letterhead)

RFP No:

(Letter to be submitted by the OEMs on their letter head)

To,

General Manager
Punjab & Sind Bank
Second Floor
IT Department
Plot Number 151, Sector 44,
Gurugram, 122003

Dear Sir,

Sub: Request for Proposal for Selection of Bidder(s) for Supply, Installation, Implementation, Maintenance and Management of _____ under RFP No. _____

We, _____, a reputed manufacturer/OEM of the products proposed under the above-mentioned RFP, having our registered office at _____ and development/manufacturing facilities at _____, hereby certify and confirm the following:

S. No.	Product Name as per RFP	Product Name as per OEM	Model	Version
1				
2				

1. We confirm that the products proposed above fully comply with the requirements specified in the RFP. The compliance against the Functional Requirement Specifications (FRS) and Technical Requirement Specifications (TRS) has been provided by us and submitted by the bidder in the prescribed format as part of the bid response.
2. We further confirm that our proposed products fully comply with the scope of work, technical specifications, service levels, interoperability requirements, support obligations, and all other applicable terms and conditions of the RFP relevant to the proposed solution.
3. We certify that the OEM make, model, and version declared herein are identical to those proposed by the bidder in the Undertaking, Technical Bid, and Masked BoM. No alternate product, model, version, equivalent offering, or substitute product has been proposed.
4. We confirm that the proposed product(s) are currently supported, commercially available, and not under End-of-Sale (EOS) status as on the bid submission date.
5. We have attached the Software Bill of Materials (SBOM) and Cybersecurity Bill of Materials (CBOM - Public) for the proposed solution in the format prescribed under Annexure 20. The detailed/private SBOM and CBOM containing confidential or sensitive security information shall be provided to the Bank after issuance of the Purchase Order and execution of applicable confidentiality requirements.
6. We further confirm that we support secure, automated, and machine-readable exchange of SBOM/CBOM information through industry-recognized formats and mechanisms and shall

facilitate the Bank in obtaining updated SBOM/CBOM information throughout the contract period.

7. We undertake to provide all necessary OEM support, software updates, security patches, vulnerability disclosures, technical advisories, and product lifecycle information for the duration of the contract.
8. We understand that any misrepresentation, incorrect declaration, or inconsistency between this declaration, the bidder's submission, the Undertaking, or the proposed products may result in rejection of the bid and/or any action deemed appropriate by the Bank.

For and on behalf of the OEM

Authorized Signatory: _____

Name: _____

Designation: _____

OEM Name: _____

Signature & Seal

Date: _____

The OEM hereby confirms that the product make, model, and version declared herein and submit by the bidder are the only products proposed under the bid. Any subsequent change, substitution, upgrade, downgrade, replacement, or introduction of an alternate product shall require prior written approval of the Bank.

15.19 Annexure 19: Stack Confirmation Sheet- Undertaking for Proposed OEM Products

(To be submitted on Bidder's Letterhead duly signed by the Authorized Signatory)

We hereby undertake that the products proposed under this bid are as detailed below. We further confirm that the details furnished herein are true and correct and shall exactly match the details provided in the Masked Bill of Materials (BoM) submitted as part of the bid.

In case of any discrepancy, inconsistency, omission, mismatch, or ambiguity between the Masked BoM and this Undertaking, the details provided in this Undertaking shall prevail for the purpose of technical evaluation and contract execution.

S. No.	Solution Name	Make / OEM Name	Product Model / Version Proposed
1	Anti-Distributed Denial of Services (Anti-DDoS)		
2	SSL Orchestrator along with packet broker		
3	DNS protection (Internal DNS Security)		
4	Web Gateway		
5	Zero-Day Attack Protection at Endpoint and network/Anti-APT		
6	Zero Trust Network Access (ZTNA)		
7	Data Loss Prevention (DLP)		
8	Information/Digital Right Management		
9	Database Activity Monitoring		
10	Mobile SDK		
11	Host IPS including Application Change Control (HIPS)		
12	Web Application Firewall (WAF)		
13	Centralized key management solution		
14	Certificate Lifecycle management		
15	Identity & Access Management Solution		
16	Multi Factor Authentication		
17	Privilege Identity/Access Management		
18	DNS Security Services (Internet-Facing DNS Security Services)		
19	Cloud Access Security broker (CASB)		
20	AI Security		
21	SBOM, CBOM, AIBOM & QBOM		

Declaration

1. We certify that all products proposed above are commercially available and supported by the respective OEMs.
2. We certify that the Make/OEM and Product Model mentioned above are identical to those quoted in the Masked BoM and shall be supplied in the event of award of contract.

3. We understand that the Bank shall evaluate the technical compliance based on the information furnished in this undertaking and supporting technical documents.
4. Any incorrect declaration, misrepresentation, substitution of OEM/model, or discrepancy between this undertaking and the submitted BoM may result in rejection of the bid and/or any other action deemed appropriate by the Bank.
5. The Bank reserves the right to seek OEM confirmation, product datasheets, licenses, authorizations, or any additional documentary evidence to validate the details furnished herein.
6. Proposing multiple options, alternate OEMs, substitute products, or equivalent solutions for any solution component is not permissible and may render the bid non-responsive and liable for rejection.

Authorized Signatory

Name: _____

Designation: _____

Bidder Name: _____

Signature & Seal: _____

Date: _____

15.20 Annexure 20: S-BOM & C-BOM DETAILS of all the proposed Tool/solutions

a. S-BOM

On OEM Letterhead

S.No.	Component	Component Name	Component Name	Component Name	Component Name	Component Name	Component Name
1.	Version						
2.	Description						
3.	Supplier						
4.	License						
5.	Origin						
6.	Dependencies						
7.	Vulnerabilities						
8.	Patch Status						
9.	Release Date						
10.	End of Life Date						
11.	Usage Restrictions						
12.	Checksums						
13.	Hashes						
14.	Executable Property						
15.	Archive Property						
16.	Structured Property						
17.	Unique Identifier						

b. C-BOM

On OEM Letterhead

S.No.	Component	Component Name	Component Name	Component Name	Component Name	Component Name	Component Name
1.	Version						
2.	Description						
3.	Supplier						
4.	License						
5.	Origin						
6.	Dependencies						
7.	Vulnerabilities						
8.	Patch Status						
9.	Release Date						
10.	End of Life Date						
11.	Usage Restrictions						
12.	Checksums						
13.	Hashes						
14.	Executable Property						
15.	Archive Property						
16.	Structured Property						
17.	Unique Identifier						

15.21 Annexure 21: Sizing/Volumetrics, Data Retention and Current Infrastructure

#	Solution Name	Volumetrics
1.	Non-Production Environment	For appliance-based solutions, the bidder shall design and propose an appropriate non-production environment to support testing, validation, upgrades, patching, configuration changes, policy tuning, rule testing, and other activities during the contract period without impacting production services. For VM-based solutions, the non-production environment shall be sized at a minimum of 10% of the Production (DC) environment unless otherwise specified in the RFP.

The bidder shall ensure that all archived logs, records, events, alerts, forensic artefacts, audit trails, and other retained data can be restored and made available in the respective native technology platform and readable format whenever required by the Bank for forensic investigations, incident response, audit, compliance, regulatory, legal, or operational purposes.

The bidder shall be solely responsible for sizing all infrastructure components required for successful deployment and operation of the proposed solution, including but not limited to compute, storage, backup, network, bandwidth, IOPS, CPU, memory, servers, operating systems, databases, virtualization, cloud resources, and associated software. Such sizing shall be carried out in consultation with the respective infrastructure OEMs and solution/service OEMs and shall account for all performance, availability, retention, security, disaster recovery, and SLA requirements specified in the RFP.

The bidder and respective OEMs shall account for the projected growth, increase in transaction volumes, security events, log generation rates, storage consumption, user base, applications, and regulatory requirements throughout the contract period while arriving at the proposed sizing. The proposed solution shall meet all functional, technical, performance, scalability, availability, security, and service level requirements during the entire contract period. Any augmentation, upgrade, expansion, or replacement required due to inadequate sizing, incorrect assumptions, or failure to account for projected growth shall be carried out at no additional cost to the Bank inline with the terms stated in Section 7.13 - IT Infrastructure.

15.21.1 Existing and Envisaged Stack:

A. Existing Solution Stack:

Perimeter Security	Perimeter Firewall	DDoS	SSLi*	Email Security	DNS	Web Gateway Appliance	Anti-APT	Remote Access VPN
Network Security	Core Next Generation Application layer Firewall		NAC					
Endpoint Security	Data Classification	MTP	DRM	DLP	MDM	Endpoint Forensic & Behavior Analysis	Endpoint Anti Phishing	Endpoint Security
Application Security	HIPS	Application Security Testing Tool	WAF					
Data Security	DAM	SDK						
Access Management	IDAM*	MFA*	PIM					
Management and Policy Layer	SIEM	TTS*	NSPM	ITGRC	Vulnerability Management			
	Decoy	NBAD						

B. Envisaged Solution that would be part of Security transformation that would be implemented/augmented in banks cyber Transformation:

Perimeter Security	Perimeter Firewall	Third Party Firewall	DDoS	SSLi	Email Security	DNS	Web Gateway Appliance	Zero Day Attack	ZTNA
Network Security	Core Next Generation Application layer Firewall								
Endpoint Security	xDR	MTP	DRM	DLP					
Application Security	HIPS	Application Security Testing Tool	WAF	Centralized Key Management	File Upload Management	CSPM	S-BOM	Anti-deepfake Solution	
Data Security	DAM	SDK							
Access Management	IDAM	MFA	PIM						
Management and Policy Layer	SIEM	SOAR	AIML UEBA	ITGRC	Threat Intelligence Platform	Vulnerability lifecycle & Management			
	Decoy		NSPM						

Integration and re-integration with the above solution is to be done by the bidder at no additional cost to the bank

15.21.2 Existing IT Security Solution Details

The bidder must ensure that the bank's investments are secured. Accordingly, the bidder is required to either replace or augment the proposed solution to comply with the requirements specified in the RFP.

#	Description	OEM MAKE	OEM MODEL
1	Distributed Denial of Services (DDoS)	Radware	Radware DefensePro 20-2
3	DNS Protection	Efficient IP	Solid Server
4	Web Gateway appliance	McAfee "Skyhigh"	MFE Web Gateway 5500 Appliances
5	Anti-Advanced Persistent Threat Protection(Anti-APT)	Trend Micro	TrendMicro Deep Discovery Appliances
6	Remote Access VPN	Array	AVX 5800 Hardware
7	Data Loss Prevention	McAfee "Trellix"	MFE DLP 6600A Appliance
8	Information / Digital Rights Management	BlackBerry	Blackberry Workspaces
9	Database Activity Monitoring	McAfee "Trellix"	MFE Data Centre SEC Suite Dbase
10	SDK for Mobile Access Security	Checkpoint	Sandblast App Protect
11	Host IPS including application change control	Trend Micro	TrendMicro Deep Security
12	Web Application Firewall (WAF)	Baracuda	WAF 660
13	Privilege Identity Management Solution (PIM)	ARCON	U16

15.21.3 Current IT assets

S.No.	Current assets description	Current assets
Centralized IT Infrastructure		
1	Servers deployed with OS, DB, Web/app component, middleware's, agents and other applications / software, private & public cloud setups, emerging technologies etc.	2500
2	Database	300
3	Intranet and internet facing business & non-business applications like CBS, Internet Banking, Mobile Banking, HRMS, O365 etc.	200
Branches		
4	Desktops with various agents like AV, DLP, NAC, ITAM etc.	12000
5	Routers & Switches	7200

Note: The count of IT & Security Infra as listed above is tentative.

15.21.4 Deployment & Data Retention

S. No.	Solution Name	Application/Solution/Appliance Deployment Requirement	Retention Requirement	Volumetrics
1	Anti-DDoS	1. Bank's DC - HA (N+N Active-Active) deployment 2. Bank's DR - HA (N+N Active-Active) deployment Solution should be designed of protecting inbound and outbound traffic at both sites.	1 Month (Logs and Data Storage on Appliance / Primary Storage)	Refer Functional Requirement sheet
2	SSL Orchestrator Tool and Packet Broker	1. Bank's DC - HA (N+N Active-Active) deployment 2. Bank's DR - HA (N+N Active-Active) deployment Solution should be designed with synchronized policies and traffic visibility.	1 Month (Logs and Data Storage on Appliance / Primary Storage)	Refer Functional Requirement sheet
3	DNS Protection	DHCP 1. Bank's DC - HA (N+N Active-Passive) deployment 2. Bank's DR - HA (N+N Active-Passive) deployment IPAM 1. Bank's DC - Standalone deployment 2. Bank's DR - Standalone deployment Recursive DNS 1. Bank's DC - HA (N+N Active-Passive) deployment 2. Bank's DR - HA (N+N Active-Passive) deployment	1 Month (Logs and Data Storage on Appliance / Primary Storage)	DHCP Volumetrics Details: a. Total Number of Client Devices (PCs, printers, IoTs) -- 35000 b. Percentage (%) of devices online at peak - 80% c. Lease Duration - 8 Hours Licenses on Day 1 is to be provided for 100000 IPs scalable to 200000 Ips

S. No.	Solution Name	Application/Solution/Appliance Deployment Requirement	Retention Requirement	Volumetrics
		- DHCP will be used for internal client networks, not in the DMZ. - Recursive DNS will be hosted in DMZ - DHCP and IPAM services will be deployed in MZ - Since DHCP and IPAM services are not required in the DMZ, bidders should propose separate components/servers (virtual or physical) for DHCP and IPAM functionalities, if their solution architecture requires them to operate separately.		
4	Web Gateway	- Bank's DC - HA (N+N Active-Active) deployment - Bank's DR - HA (N+N Active-Active) deployment Solution should be designed with centralized policy, reporting, and threat intelligence.	1 Month (Logs and Data Storage on Appliance / Primary Storage)	Users: 12000 Scalable to 16000
5	Zero-Day Attack Protection for Endpoint and Network	- Bank's DC - HA (N+N Active-Active) deployment - Bank's DR - HA (N+N Active-Active) deployment - The sandboxing environment - HA (N+N Active-Passive) deployment at DC - HA (N+N Active-Passive) deployment at DR	1 Month (Logs and Data Storage on Appliance / Primary Storage)	Endpoints: 12000 Scalable to 16000 Throughput Handling - 10 Gbps of traffic capacity
6	ZTNA	Bank's DC - HA (N+N Active-Active) deployment	1 Month (Logs and Data Storage on Primary Storage)	User: 250 users scalable to 500

S. No.	Solution Name	Application/Solution/Appliance Deployment Requirement	Retention Requirement	Volumetrics
		2. Bank's DR - HA (N+N Active-Active) deployment 3. Dedicated ZTNA Management and Policy Controller to be provided separately: a. HA (N+N Active-Active) deployment at both DC and DR, or b. HA (N+N Active-Active) deployment at Cloud-hosted (where OEM architecture mandates SaaS management)		
7	DLP	1. Bank's DC - HA (N+N Active-Active) deployment 2. Bank's DR - HA (N+N Active-Active) deployment Dedicated DLP Policy Management, Incident Management and Reporting Server a. Standalone at DC b. Standalone at DR Solution should be designed with centralized policy management, incident management, and reporting.	1 Month (Logs and Data Storage on Primary Storage)	12000 Users scalable to 16000
8	Information/ Digital Rights Management	1. Bank's DC - HA (N+N Active-Active) deployment 2. Bank's DR - HA (N+N Active-Active) deployment	1 Month (Logs and Data Storage on Appliance / Primary Storage)	Admin/Policy & Rules Creator License for 200 users. Any number of users can apply the created policy if provided access to by admin.
9	Database Activity Monitoring	1. Bank's DC - HA (N+N Active-Active) deployment	1 Month (Logs and Data Storage on Appliance / Primary Storage)	150 Applications Database at DC and 150 Application Database at DR

S. No.	Solution Name	Application/Solution/Appliance Deployment Requirement	Retention Requirement	Volumetrics
		2. Bank's DR - HA (N+N Active-Active) deployment		
10	Mobile SDK	1. Bank's DC - HA (N+N Active-Active) deployment 2. Bank's DR - HA (N+N Active-Active) deployment 3.	1 Month (Logs and Data Storage on Appliance / Primary Storage)	Users Count- 15,00,000 (Day 1) scalable to 30,00,000
11	HIPS	1. Bank's DC - HA (N+N Active-Active) deployment 2. Bank's DR - HA (N+N Active-Active) deployment 4.	1 Month (Logs and Data Storage on Primary Storage)	3000 VMs/Servers scalable to 4500 VMs/Server
12	WAF	1. Bank's DC - HA (N+N Active-Active) deployment 2. Bank's DR - HA (N+N Active-Active) deployment	1 Month (Logs and Data Storage on Appliance / Primary Storage)	Refer Functional Requirement sheet
13	Centralised Key Management	1. Bank's DC - HA (N+N Active-Active) deployment 2. Bank's DR - HA (N+N Active-Active) deployment	1 Month (Logs and Data Storage on Appliance / Primary Storage)	Enterprise-Wide licenses
14	Certificate Lifecycle Management	1. Bank's DC - HA (N+N Active-Active) deployment 2. Bank's DR - HA (N+N Active-Active) deployment	1 Month (Logs and Data Storage on Appliance / Primary Storage)	Enterprise-wide licenses for Certificate Issuance, provisioning and management

S. No.	Solution Name	Application/Solution/Appliance Deployment Requirement	Retention Requirement	Volumetrics
15	IDAM	1. Bank's DC - HA (N+N Active-Active) deployment 2. Bank's DR - HA (N+N Active-Active) deployment	1 Month (Logs and Data Storage on Appliance / Primary Storage)	12000 scalable to 16000
16	MFA	1. Bank's DC - HA (N+N Active-Active) deployment 2. Bank's DR - HA (N+N Active-Active) deployment	1 Month (Logs and Data Storage on Appliance / Primary Storage)	12000 scalable to 16000
17	PIM	1. Bank's DC - HA (N+N Active-Active) deployment 2. Bank's DR - HA (N+N Active-Active) deployment	1 Month (Logs and Data Storage on Appliance / Primary Storage)	1. User Licenses: 750 User (Day 1) scalable to 1500 2. Services Licenses - 3000 service (Day 1) scalable to 4500
18	DNS Security Services (Internet)	1. Cloud-based DNS Security Service with High Availability integrated with the Bank's DNS infrastructure. 2. On-Premises solution 2.1. Bank's DC - HA (N+N Active-Active) deployment 2.2. Bank's DR - HA (N+N Active-Active) deployment	1 Month (Logs and Data Storage on Appliance / Primary Storage)	20 Domains of PSB
19	S-BOM, C-BOM, AI-BOM & QBOM	1. Standalone at DC 2. Standalone at DR	1 Month (Logs and Data Storage on Appliance / Primary Storage)	Applications – 50 scalable to 150 HSM – 16 Qty 10 AI Applications

S. No.	Solution Name	Application/Solution/Appliance Deployment Requirement	Retention Requirement	Volumetrics
20	AI Security	1. Bank's DC - HA (N+N Active-Active) deployment 2. Bank's DR - HA (N+N Active-Active) deployment	1 Month (Logs and Data Storage on Appliance / Primary Storage)	Business Users - 12000 scalable to 16000 Enterprise AI Applications- 10 Qty AI Models- Unlimited AI Users - Unlimited Prompts- Unlimited API Calls- Unlimited AI Sessions- Unlimited AI Policies- Unlimited
21	CASB	1. Bank's DC - HA (N+N Active-Active) deployment 2. Bank's DR - HA (N+N Active-Active) deployment	1 Month (Logs and Data Storage on Appliance / Primary Storage)	Cloud Users– 50 users scalable to 100 users
22	Backup & Retention (Provided and maintained by bank)	Centralized Backup & Retrieval Solution deployed across DC and DR. Solution shall support automated backup, replication, indexing, retrieval, and immutable archival of all logs, alerts, events, configurations, reports, incidents, and security artefacts generated by all proposed solutions.		Bidder to right size

Retention Requirement:

Backup Type	Retention Location	Retention Period
Daily Incremental Backup	Backup Storage / Backup Appliance	1 Weeks
Weekly Full Backup	Backup Storage / Backup Appliance	2 Weeks
Monthly Full Backup	Backup Storage / Backup Appliance	2 Months
Monthly Full Backup (Post Retention Period)	Long-Term Storage (LTS)	Entire Duration of the Contract

Note: The proposed Backup and Retrieval Solution shall be sized to support the above retention policy. Upon completion of the two (2) month retention period on Backup Storage, Monthly Full Backups shall be migrated to Long-Term Storage (LTS) and retained in immutable Write Once Read Many (WORM) format for the entire contract period.

The proposed Primary, backup Storage and Long-Term Storage (LTS) shall be adequately sized not only to meet the prescribed backup and retention requirements but also to support data restoration, retrieval, search, and forensic investigation activities. The bidder shall ensure that all backed up and archived data, logs, configurations, reports, videos, and other artefacts remain recoverable, readable, and accessible throughout the applicable retention period without impacting operational or regulatory requirements.

15.22 Annexure 22: Client References Format

Format for Submission of Client References

To whosoever it may concern

Particulars	Details
Supporting Documents (Mandatory)	As per the Criteria
Additional Documentary Evidence (Any One Mandatory)	As per the Criteria
Client Information	
Client Name	
Client Address	
Name of Contact Person & Designation	
Contact Number of Contact Person	
Email Address of Contact Person	
Project Information	
Name of the Project	
Project Location	
Start Date of Project	
End Date of Project (if completed)	
Current Project Status	☐ Completed ☐ In Progress
Industry / Sector	
Project Size & Commercials	
Value of Single Work Order / Contract (INR Lakhs)	
Number of Branches / Offices Covered	
Scope of Work	
Brief Description of Scope Relevant to PSB Requirement	

Cyber Security Solutions Implemented (Tick Applicable Solutions)	
Anti-Distributed Denial of Services (Anti-DDoS)	☐ Yes ☐ No
SSL Orchestrator along with packet broker	☐ Yes ☐ No
DNS protection (Internal DNS Security)	☐ Yes ☐ No
Web Gateway	☐ Yes ☐ No
Zero-Day Attack Protection at Endpoint and network/Anti-APT	☐ Yes ☐ No
Zero Trust Network Access (ZTNA)	☐ Yes ☐ No
Data Loss Prevention (DLP)	☐ Yes ☐ No
Information/Digital Right Management	☐ Yes ☐ No
Database Activity Monitoring	☐ Yes ☐ No
Mobile SDK	☐ Yes ☐ No
Host IPS including Application Change Control (HIPS)	☐ Yes ☐ No
Web Application Firewall (WAF)	☐ Yes ☐ No
Centralized key management solution	☐ Yes ☐ No
Certificate Lifecycle management	☐ Yes ☐ No
Identity & Access Management Solution	☐ Yes ☐ No
Multi Factor Authentication	☐ Yes ☐ No
Privilege Identity/Access Management	☐ Yes ☐ No
DNS Security Services (Internet-Facing DNS Security Services)	☐ Yes ☐ No
Cloud Access Security broker (CASB)	☐ Yes ☐ No
AI Security	☐ Yes ☐ No

SBOM, CBOM, AIBOM & QBOM	☐ Yes ☐ No
Evidence Submitted	
Copy of PO / WO / Contract Attached	☐ Yes ☐ No
Client Credential Letter / Email Attached	☐ Yes ☐ No
Client Installation Report / Sign-off Attached	☐ Yes ☐ No
OEM Self-Declaration Attached	☐ Yes ☐ No
Additional Documents Submitted	
Clause-to-Evidence Mapping Matrix	
Document Type (PO/Contract/Credential Letter/Email/OEM Declaration)	
Page Number in the proposal	
Section Number in the proposal	
Sub-Section / Clause No. in the proposal	
Exact Relevant Excerpt from the document type	
Certification by Bidder	We hereby certify that the above information is true and correct and supported by documentary evidence submitted as part of the bid.
Authorized Signatory Name	
Designation	
Signature & Seal	
Date	

15.23 Annexure 23: Pre-bid Query format

Pre-Bid Query Format

(Bidders should submit the queries in excel format only)

Ref: RFP No. _____ dated _____.

Bidder's Name: _____

S.No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query
1					
2					
3					
4					
5					
-					

15.24 Annexure 24: Proposed Resources CV

Sr No	Parameter	Description	
1	Name & Designation		
2	Proposed Position & Skillset		
4	Educational Qualification		
	Degree Obtained	University/ Institution	Year Obtained
5	Cybersecurity Certification/Qualifications		
6	Professional Experience		
	Designation	Company Name	Year Obtained
7	Total Years of Cyber Security Experience		
8	IT Security Solution and the relevant Project from the below solution 1. Anti-Distributed Denial of Services (Anti-DDoS) 2. SSL Orchestrator along with packet broker 3. DNS protection (Internal DNS Security) 4. Web Gateway 5. Zero-Day Attack Protection at Endpoint and network/Anti-APT 6. Zero Trust Network Access (ZTNA) 7. Data Loss Prevention (DLP) 8. Information/Digital Right Management 9. Database Activity Monitoring 10. Mobile SDK 11. Host IPS including Application Change Control (HIPS)		

	12. Web Application Firewall (WAF) 13. Centralized key management solution 14. Certificate Lifecycle management 15. Identity & Access Management Solution 16. Multi Factor Authentication 17. Privilege Identity/Access Management 18. DNS Security Services (Internet-Facing DNS Security Services) 19. Cloud Access Security broker (CASB) 20. AI Security 21. SBOM, CBOM, AIBOM & QBOM	
10	Experience relevant to the Project Wise	

15.25 Annexure 25: Insurance Surety Bond against EMD

(To be executed on Non-Judicial Stamp Paper of Appropriate value)

Insurance Surety Bond No..... Date:.....

(Name of the RFP:)

To: (Name and address of The Beneficiary/ Bank)

WHEREAS (Name of Bidder) (hereinafter called "the Bidder") has submitted its Bid dated (date of bid) for the Earnest Money Deposit for the captioned RFP _____ (hereinafter called "the Bid") KNOW ALL PERSONS by these present that We (name of Insurance Company) (address of Insurance Company) (hereinafter called "the Surety"), are bound unto Punjab & Sind Bank, _____, constituted under the provisions of Banking Companies (Acquisition & Transfer of Undertakings) Act, 1970, having its Head Office at Punjab & Sind Bank, IT Department, Plot No. 151, Sector 44, Gurugram, 122003, hereinafter called "the Beneficiary/ Bank") for the sum of..... (amount), for which payment well and truly to be made to the said Beneficiary/ Bank, the Surety binds itself, its successors and assigns by these presents.

THE CONDITIONS of this obligation are as follows:

1. If the Bidder (a) withdraws or modifies its Bid during the period of bid validity, or (b) adopts corrupt or collusive or coercive or fraudulent practices or defaults under Integrity Pact.
2. If the Bidder, having been notified of the acceptance of its Bid by the Beneficiary/ Bank during the period of bid validity.
 - a. fails or refuses to sign the Contract Agreement when required, or
 - b. fails or refuses to submit the performance security in accordance with the Tender Documents.

We undertake to pay to the Beneficiary/ Bank up to the above amount upon receipt of its first written demand, without the Beneficiary/ Bank having to substantiate its demand, provided that in its demand the Beneficiary/

Bank will mention that the amount claimed by it is due, owing to the occurrence of one or both of the two above-named CONDITIONS, and specifying the occurred condition or conditions.

The Surety declares that this Insurance Surety Bond is issued by the..... (name of Insurance Company) as per the applicable rules and regulations of Insurance Regulatory Development Authority of India (IRDAI).

This Insurance Surety Bond will remain in force up to and including (date 90 days after the period of bid validity), and any demand in respect thereof must reach the Surety not later than the above date.

INSTRUCTIONS FOR EXECUTION OF INSURANCE SURETY BOND FOR EARNEST MONEY DEPOSIT

1. Insurance Surety Bond for Earnest Money Deposit should be executed on non-judicial Stamp papers of requisite value in accordance with the stamp Act if applicable to that particular state of Indian Union country of executing Insurance Company, where executed. In case the same is issued by an International Insurance Company (it should be registered under insurance Act 1938 or as amended from time to time and approved by the Insurance Regulatory Development Authority of India (IRDAI)) the law prevalent in the country of execution shall prevail for the purpose of Stamp Duty on the Insurance Surety Bond. However, in such a case, the Insurance Surety Bond for Earnest Money Deposit shall be got confirmed by the Bidder through any Indian Scheduled/Nationalized Insurance Company.
2. The executing officers of the Insurance Surety Bond for Earnest Money/Bid Security shall clearly indicate in (block letters) his name, designation, Power of Attorney No./Signing Power No. as well as telephone/ fax numbers with full correspondence address of the issuing Guarantee etc.
3. Each page of the Insurance Surety Bond for Earnest Money Deposit shall be duly signed/initialled by the executing officers and the last page shall be signed in full, indicating the particulars as aforesaid (sub-para 2) under the seal of the Insurance Company.
4. Stamp paper shall be purchased in the name of Insurance Company counting the Insurance Surety Bond, after the date 'Notice Inviting Tender', not more than six months prior to execution/issuance of the Insurance Surety Bond. The name of the purchaser should appear at the back side of stamp paper in the Vendors Sign. The issuing insurance Company shall be requested independently for

verification/confirmation of the Insurance Surety Bond issued, non-confirmation of which may lead to rejection of 'Insurance Surety Bond'

5. Irrevocable, valid and fully enforceable Insurance Surety Bond in favour of the Beneficiary/ Bank (Name of Beneficiary/ Bank) issued by any Insurance Company registered under Insurance Act amended from time to time and approved by the Insurance Regulatory Development Authority of India (IRDAI) in Indian currency (INR) only is acceptable to the Beneficiary/ Bank.
6. Insurance Surety and for Bid security in original shall be submitted along with the Bid. However, the Issuing Insurance Company shall submit an unstamped duplicate copy of Insurance Surety Bond directly by registered post (A.D.) to the Beneficiary/ Bank (authority inviting tenders) with forwarding letter.

or and on behalf of the Insurance Company
in the capacity of

Common Seal of the Insurance Company with complete address including Tel. Nos./e-Mail Id. Staff Authority No. of the officer of the Insurance Company/Signatory.