

PUNJAB & SIND BANK



REQUEST FOR PROPOSAL

FOR

**SELECTION OF BIDDER FOR SUPPLY INSTALLATION, IMPLEMENTATION,
MAINTENANCE & MANAGEMENT OF IT SECURITY SOLUTIONS - B**

BID NO: PSB/HOIT/RFP/2025-26/45 DATED 01/10/2025

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

TABLE OF CONTENTS

TABLE OF CONTENTS.....	3
1 KEY INFORMATION	8
2 GLOSSARY	11
3 DISCLAIMER	15
4 INTRODUCTION.....	16
5 PROJECT OBJECTIVE.....	16
6 INSTRUCTION TO BIDDER	17
6.1 Cost of Tender	17
6.2 Language of the Bid	17
6.3 Bid Currency & Price Structure	17
6.4 Bid System Offer.....	17
6.5 Two Bid System:	18
6.5.1 Preparation of Bids:	18
6.6 Cost of Preparation.....	19
6.7 Normalization of Bids	19
6.8 Submission of Bid and communication	19
6.9 Late bids	20
6.10 Modifications and/ or Withdrawal of Bids	20
6.11 Earnest Money Deposit (EMD):	21
6.12 Performance Bank Guarantee/Security Deposit (PBG)	22
6.13 No commitment to accept lowest or any bid.....	22
6.14 Right To Accept Any Bid and To Reject Any OR All Bids/Cancellation of Tender process 23	
6.15 Correction of Errors	23
6.16 Soft copy of tender document	24
6.17 Bid validity period	24
6.18 Pre-bid meeting.....	24
6.19 Amendment to RFP Contents	25
6.20 Disqualification	25
6.21 Fixed Price	25
6.22 Project Execution	25
6.23 Confidentiality of the Bid Document.....	25
7 SCOPE OF WORK.....	26

7.1	RACI (Responsible, Accountable, Consulted, Informed).....	29
7.2	Functional Requirements.....	29
7.2.1	Endpoint Security	29
7.2.2	Application Security.....	31
7.2.3	Data Security.....	34
7.2.4	Management Layer Security	37
7.3	Migration - Activities are to be performed by Respective solution OEM (supported by bidder) 43	
7.4	Non-functional requirements.....	45
7.5	Security requirements - Activities are to be performed by Respective solution OEM (supported by bidder)	46
7.6	IT Infrastructure requirements.....	47
7.6.1	Compute Infrastructure	50
7.6.2	Storage Infrastructure – Primary & Object	51
7.6.3	Backup Infrastructure	51
7.6.4	Software.....	52
7.7	Other requirements	52
7.7.1	Requirement Analysis - Activities are to be performed by Respective Solution OEM (supported by bidder).....	53
7.7.2	System Design - Activities are to be performed by Respective solution OEM (supported by bidder).....	54
7.7.3	Development and Installation - Activities are to be performed by Respective solution OEM (supported by bidder).....	55
7.7.4	Documentation - Activities are to be performed by Respective solution OEM (supported by bidder).....	56
7.7.5	Deployment and Go-Live - Activities are to be performed by Respective Solution OEM (supported by bidder).....	57
7.7.6	Testing- Activities are to be performed by Respective solution OEM (supported by bidder) 58	
7.7.7	Training- Activities are to be performed by Respective solution OEM (supported by bidder) 64	
7.8	ATS and AMC.....	64
7.9	Resource Requirement	65
7.10	Facilities Management.....	70
7.10.1	Continual Improvement	70
7.10.2	DR Drill.....	73
7.10.3	IT Security operations:	73

7.10.4	OEM Services & Deployment: (Architecture assessment)	80
7.10.5	System recovery	81
7.11	Other In-Scope services.....	82
7.11.1	Other Scope Activity.....	82
7.11.2	Escrow	83
7.11.3	Exit Plan Management.....	83
7.11.4	Security Management	84
7.11.5	DR Setup - Activities are to be performed by Respective solution OEM (supported by bidder) 85	
8	CONTRACT PERIOD	86
9	PROJECT TIMELINES	86
10	EVALUATION CRITERIA.....	87
10.1	Preliminary Scrutiny.....	87
10.2	Eligibility Evaluation Criteria.....	89
10.3	Technical Evaluation Criteria	94
10.4	Commercial Evaluation Criteria	98
10.5	Final Evaluation – Weighted Techno-Commercial Evaluation	98
11	PAYMENT TERMS.....	100
11.1	Product (Software) Cost.....	100
11.2	OEM Services Cost	101
11.3	Hardware Cost	101
11.4	ATS/subscription cost & AMC Cost.....	102
11.5	Facility Management (FM) Cost:	102
11.6	Other Cost	102
12	SERVICE LEVELS & PENALTIES.....	104
12.1	Service Level Agreement.....	104
12.2	Penalties	114
12.3	At-Risk Amount	115
13	TERMS AND CONDITIONS	116
13.1	Assignment & Subcontracting	116
13.2	Delays in the Bidder's Performance.....	116
13.3	Jurisdiction.....	116
13.4	Dispute Resolution	116
13.5	Notices	116
13.6	Authorized Signatory.....	117

13.7	Make in India	117
13.8	Confidentiality.....	117
13.9	Indemnity.....	118
13.10	Force Majeure	118
13.11	Ownership & Retention of Documents:.....	118
13.12	Conflict of Interest:.....	119
13.13	Signing of Pre-Contract Integrity Pact:	119
13.14	Liquidated Damages	119
13.15	Intellectual Property Indemnity:	120
13.16	Limitation of Liability.....	120
13.17	Order Cancellation	120
13.18	Consequences of Termination	121
13.19	Audit by Third Party	122
13.20	Access Through Virtual Private Network (VPN)	123
14	APPENDIX	124
14.1	APPENDIX 1A: Functional Compliance Sheet:.....	124
14.2	APPENDIX 1B: Technical Compliance Sheet	124
14.3	APPENDIX 2: Commercial Bill of material Sheet.....	124
14.4	APPENDIX 3: Bill of Quantity.....	124
15	ANNEXURES	125
15.1	Annexure 1: Submission Checklist (on bidder's letterhead)	125
15.2	Annexure 2: Bidder's Information	126
15.3	Annexure 3: Tender Covering Letter	129
15.4	Annexure 4: Bid Security Declaration.....	131
15.5	Annexure 5: Pre-Qualification Criteria	133
15.6	Annexure 6: Acceptance/Compliance Certificate	134
15.7	Annexure 7: Manufacturer's Authorization Form	135
15.8	Annexure 8: Certification on OEM Requirements.....	137
15.9	Annexure 9: Escalation Matrix	139
15.10	Annexure 10: Litigation Certificate.....	140
15.11	Annexure 11: Non-blacklisting undertaking.....	141
15.12	Annexure 12: Undertaking of Authenticity (on bidder's letterhead)	142
15.13	Annexure 13: Non-Disclosure Agreement	143
15.14	Annexure 14: Commercial Proposal Submission Checklist.....	148
15.15	Annexure 15: Bank Guarantee Format for Earnest Money Deposit.....	149

15.16	Annexure 16: Format of Performance Guarantee	151
15.17	Annexure 17 : Pre-contract integrity pact	154
15.18	Annexure 18: Compliance with FRS, TRS, SoW & SBOM (on respective OEM letterhead)	159
15.19	Annexure 19: Stack Confirmation Sheet.....	161
15.20	Annexure 20: S-BOM & C-BOM DETAILS of all the proposed Tool/solutions	162
15.21	Annexure 21: Sizing/Volumetrics	164
15.22	Annexure 22: Client References Format.....	167
15.23	Annexure 23: Pre-bid Query format.....	169
15.24	Annexure 24: Proposed Resources CV	170
15.25	Annexure 25: Minimum Local Content Certification	172

1 KEY INFORMATION

Particulars	Details
Tender Title	Selection of Bidder for Supply Installation, Implementation, Maintenance & Management of IT Security Solutions and Services – B
Security Deposit/Earnest Money deposit	<p>Rs. 2.9 Cr (INR Two crores and ninety lakhs only)</p> <p>Note: - Bidders who are eligible for EMD (Earnest Money Deposit) exemption as per GeM General Terms and Conditions (GeM 4.0, Version 1.25, dated 14th July 2025, Page 19) are required to submit a Bid Security Declaration in lieu of EMD.</p> <p>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.</p> <p>Failure to submit the Bid Security Declaration (where applicable) will result in the bid being treated as non-responsive.</p>
Bid validity	180 days from the date of opening of the bid.
Performance Bank Guarantee	<p>5% of Project Cost</p> <p>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</p>
Date of Publishing the tender on Bank's Website	01/10/2025
Last Date for submission of Pre-Bid Query	<p>08/10/2025</p> <p>a) Pre bid queries should be submitted as per Annexure 23 in MS- excel format.</p> <p>b) Queries must be mailed to hoit.tenders@psb.co.in only quoting tender reference number in the subject. Subject of the email should be given as “Pre-Bid Queries for PSB/HOIT/RFP/2025-26/45 DATED 01/10/2025”</p> <p>c) “. Queries reaching afterwards will not be entertained.</p>
Date and Time for Pre-Bid Meeting	<p>09/10/25 at 3:00 PM</p> <p>Pre-Bid meeting will be held Online, and participants are requested to attend the meeting Online.</p> <p>Those who are interested in participating the Prebid meeting should share the participant details to hoit.tenders@psb.co.in</p>

	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	22/10/2025 at 3:00 PM
Date and Time of Opening of Bids	22/10/2025 at 3:30 PM
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, 2 nd Floor, Plot No. 151, Sector 44, Institutional Area, Gurugram -122003.
Contact Persons for any clarifications/ Submission of Bids	1. Mr. Nilesh Kanphade – AGM (IT) nilesh.k@psb.co.in +91 9868456224 2. Mr. Nishant Kapoor Sr. Manager Nishant.kapoor@psb.co.in +91 9569958678 3. Mr. Pawan Kumar Pawan.kumar1@psb.co.in +91 7018956787
Project Office Location	Punjab & Sind Bank Head Office: HO IT, 2 nd Floor, Plot No. 151, Sector 44, Institutional Area, Gurugram -122003.
	1. Subsequent changes made based on the suggestions and clarifications as per pre-bid meeting shall be deemed to be part of the RFP document and shall be shared with all the bidders. 2. No suggestions or queries shall be entertained after pre-bid meeting. 3. This document can be downloaded from following website: https://punjabandsind.bank.in & www.eprocure.gov.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). 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:	
1. Purchase of RFP document including all Annexures.	
2. Addendums to the RFP.	
3. Submission of Technical Bid & Commercial Bid by the Bidder.	
4. Opening of Technical Bid & Commercial Bid by the Bank.	

5. Announcement of results, if any.

Instructions:

1. Bidders who wish to participate will have to register with GeM Portal and follow respective guidelines.

In case of any clarification/ queries regarding online registration/ participation, Bidders may reach out to: Email: hoit.tenders@psb.co.in

* All MSEs(Micro & Small Enterprises) 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 Participation Fee, 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 waiting 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 glitch, 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

S.No	Acronym	Abbreviation
1	AMC	Annual Maintenance Contract
2	APT	Advanced Persistent Threat
3	ATS	Automated Testing Suite
4	BFSI	Banking, Financial Services, and Insurance
5	CBOM	Configured Bill of Materials
6	CCIL	Clearing Corporation of India Ltd
7	CEH	Certified Ethical Hacker
8	CIS	Center for Internet Security
9	CISA	Cybersecurity and Infrastructure Security Agency
10	CISA	Cybersecurity and Infrastructure Security Agency
11	CISM	Certified Information Security Manager
12	CISO	Chief Information Security Officer
13	CISSP	Certified Information Systems Security Professional
14	CK	Cyber Kill Chain
15	CPU	Central Processing Unit
16	CVE	Common Vulnerabilities and Exposures
17	CVE	Common Vulnerabilities and Exposures
18	DAM	Database Activity Monitoring
19	DB	Database
20	DC	Domain Controller
21	DDoS	Distributed Denial of Service
22	DFP	Data Flow Protection
23	DIC	District Industries Centre
24	DIPP	Department for Promotion of Industry and Internal Trade
25	DRM	Information/Digital Rights management
26	DLP	Data Loss Prevention
27	DMARC	Domain-based Message Authentication, Reporting & Conformance
28	DNS	Domain Name System
29	DPDP	Digital Personal Data Protection (Act)
30	DR	Disaster Recovery
31	DRC	Disaster Recovery Center
32	DSS	<i>Data Security Standard</i>
33	DSS	Data Security Standard
34	EMD	Earnest Money Deposit
35	FC	Fibre Channel
36	FM	Facilities Management
37	FRD	Functional Requirements Document
38	FRSM	Functional Requirements Specification Matrix

S.No	Acronym	Abbreviation
39	FTP	File Transfer Protocol
40	GCIA	GIAC Certified Intrusion Analyst
41	GDPR	General Data Protection Regulation
42	GOI	Government of India
43	GOI	Government of India
44	GST	Goods and Services Tax
45	GUI	Graphical User Interface
46	HA	High Availability
47	HIPAA	Health Insurance Portability and Accountability Act
48	HIPS	Host-based Intrusion Prevention System
49	HLD	High-Level Design
50	HO	Head Office
51	IT GRC	Information Technical Governance risk and Compliance
52	IDAM	Identity and Access Management
53	IOPS	Input/Output Operations Per Second
54	ISO	International Organization for Standardization
55	ITSM	IT Service Management
56	KMS	Centralized Key management solution
57	KVIB	Khadi and Village Industries Board
58	KVIC	Khadi and Village Industries Commission
59	LAN	Local Area Network
60	LD	Liquidated Damages
61	LDAP	Lightweight Directory Access Protocol
62	LLD	Low-Level Design
63	LOI	Letter of Intent
64	MIS	Management Information System
65	MTBF	Mean Time Between Failures
66	MTTD	Mean Time to Detect
67	MTTR	Mean Time to Resolve/Repair
68	Mobile SDK	Mobile Software Defined Kit
69	MFA	Multi- Factor Authentication
70	NAC	Network Access Control
71	NDA	Non-Disclosure Agreement
72	NEFT	National Electronic Funds Transfer
73	NGFW	Next Generation Firewall
74	NGFW	Next Generation Firewall
75	NIST	National Institute of Standards and Technology
76	NPCI	National Payments Corporation of India
77	NSIC	National Small Industries Corporation
78	NSPM	National Security Policy Management
79	OD	Overdraft
80	OEM	Original Equipment Manufacturer

S.No	Acronym	Abbreviation
81	OM	Operations Manual (or Order Management in some contexts)
82	OS	Operating System
83	OS	Operating System
84	OWASP	Open Web Application Security Project
85	OWASP	Open Web Application Security Project
86	PAM/PIM	Privileged Access Management/ Privileged identity management
87	PAN	Permanent Account Number
88	PBG	Performance Bank Guarantee
89	PCAP	Packet Capture
90	PIM	Privileged Identity Management
91	PSU	Public Sector Undertaking
92	RACI	Responsible, Accountable, Consulted, Informed (matrix)
93	RBI	Reserve Bank of India
94	RCA	Root Cause Analysis
95	RDBMS	Relational Database Management System
96	RDP	Remote Desktop Protocol
97	RFP	Request for Proposal
98	RPO	Recovery Point Objective
99	RTO	Recovery Time Objective
100	SAN	Storage Area Network
101	SANS	SysAdmin, Audit, Network, and Security Institute
102	SBOM	Software Bill of Materials
103	SCD	Software Configuration Document
104	SFG	Secure File Gateway
105	SFMS	Structured Financial Messaging System
106	SFTP	Secure File Transfer Protocol
107	SIEM	Security Information and Event Management
108	SIT	System Integration Testing
109	SIT	System Integration Testing
110	SLA	Service Level Agreement
111	SOAP	Simple Object Access Protocol
112	SOC	Security Operations Center
113	SOD	Segregation of Duties
114	SPOC	Single Point of Contact
115	SRS	Software Requirements Specification
116	SRS	Software Requirements Specification
117	SSH	Secure Shell
118	SSL	Secure Sockets Layer
119	ST	System Testing
120	TCP	Transmission Control Protocol
121	TDS	Tax Deducted at Source
122	UAT	User Acceptance Testing

S.No	Acronym	Abbreviation
123	UAT	User Acceptance Testing
124	UDP	User Datagram Protocol
125	UEM	Unified Endpoint Management
126	UNIX	Uniplexed Information and Computing System
127	USB	Universal Serial Bus
128	VAPT	Vulnerability Assessment and Penetration Testing
129	VPC	Virtual Private Cloud
130	VPN	Virtual Private Network
131	VPN	Virtual Private Network
132	WAF	Web Application Firewall
133	XDR	Extended Detection and Response
134	XML	Extensible Markup Language
135	ZTA	Zero Trust Architecture
136	ZTNA	Zero Trust Network Access

3 DISCLAIMER

- The information contained in this Request for Proposal (RFP document) or any information provided subsequently to Bidder(s) whether verbally or 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- The provisions of this Agreement 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.

4 INTRODUCTION

Punjab & Sind Bank, a body corporate constituted under the Banking Companies (Acquisition and Transfer of Undertakings) Act, 1980, one of the nationalized banks of India, has a national presence through a widespread network of 1607 branches, 29 Zonal Offices, 74 Departments in Head Office, 3 Regional Clearing Centers and 12 Currency Chests all networked under Centralized Banking Solution. It also has a network of 1000 ATMs spread across the country including onsite and offsite ATMs. With more than 116 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 frontrunner in implementing various IT enabled products.

5 PROJECT OBJECTIVE

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

This RFP invites technically mature bidder's and scalable, & interoperable solutions that will enable the Bank to establish a multi-layered defence posture covering Perimeter Security, Network Security, Endpoint Security, Application Security, Data Security at centralized level.

The bidder has to quote the prices as per Appendix 2: Commercial Bill of material. If required, the bank will procure software/ hardware/services in line with the terms and conditions defined in the RFP as per unit cost mentioned in Bill of material.

For this purpose, The Bank invites bids as per the specifications indicated in Functional and Technical Specifications and Scope of work mentioned in the RFP document. These prices shall remain valid for all orders placed with the selected bidder for the entire contract period and duly accepted by the bidder. The interested bidders are requested to send your technical proposal and Commercial proposal as per the enclosed formats.

The methodology for submission of the proposals is enumerated in Section 6: Instruction to the bidders. Terms and Conditions of Contract (TCC) are given in Section 13.

This request for proposal document ('RFP document' or RFP) has been prepared solely for the purpose of enabling Punjab and Sind Bank (hereinafter referred to as the 'BANK') For Selection of Bidder for Supply Installation, Implementation, Maintenance & Management of IT Security Solutions and Services

This invitation of Bids is limited to bidder(s) having presence in India or their Authorized Representative in India, provided firms fulfill the minimum qualification criteria.

The successful bidders would be selected, prices would be finalized through this RFP process and an agreement would be entered into with the successful bidder/s.

6 INSTRUCTION TO BIDDER

6.1 Cost of Tender

The tender document may also be downloaded from the Bank's official website <https://punjabandsind.bank.in>. The bidder downloading the tender document from the website is required to submit a non-refundable fee online as mentioned in Key-Information in favor of PUNJAB & SIND BANK, (Bank a/c details given in Key Information) before the last date and time of submission of bid, failing which the bid of the concerned Bidder will be rejected. It may be noted that the amount will not be refunded to any prospective bidder under any circumstances including cancellation of RFP.

6.2 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.

6.3 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.

6.4 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 Xerox 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 price 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.

6.5 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 1A: Functional Compliance Sheet, Appendix 1B: Technical Compliance Sheet and Appendix 3: Bill of Quantity.

Part B-Commercial Bid: Furnishing all relevant information as required as per Bill of Material as per Appendix 2. The format for submission of Commercial bid is as per Annexure 14.

6.5.1 Preparation of Bids:

6.5.1.1 Part A – Technical cum Eligibility Proposal

1. Before submitting the bid, the bidders should ensure that they 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 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 technical information as per the format given in the offer.
5. The Bank shall not allow / permit changes in the technical/functional requirements once it is submitted.
6. The relevant solution information, brand, and solution offered, printed product brochure, technical/functional specification sheets etc. should be submitted along with the Offer. Failure to submit this information along with the offer may result in disqualification.
7. The Technical Proposal should be complete in all respects and contain all the information sought for. Masked Bill of Material must be attached in Technical Offer and should not contain any price information. The Part A - Technical cum Eligibility Proposal should be complete and should cover all products and services. Technical Proposal without masked Bill of Materials will be liable for rejection. Masked Bill of Material which is not as per instruction will make Bid liable for rejection. Masked bill of material should be a replica of actual Bill of Material except that it should not contain any price information (with Prices masked). It should not provide any price information like, unit price, tax percentage, tax amount etc.

6.5.1.2 Part B - Commercial Bid

1. Commercial Bid should be submitted as per instruction in Annexure 14.
2. Commercial Bid shall be submitted as per Bill of Material and other terms and conditions of RFP on prices. The Commercial Bid should give all relevant price information as per Appendix 2. Any deviations from the Bill of Material / non submission of prices as per the format shall make the bid liable for rejection.
3. The bidder must quote the best competitive price in the commercial bid.
4. The bid must be made in an organized and structured manner.

*Note: All Claims made by the Bidder will have to be backed by documentary evidence. The bidder is expected to examine all instructions, forms, terms and specifications in the RFP. Failure to furnish all the information required or to submit a Bid not substantially responsive to the RFP in every respect will be at the Bidder's risk and may result in the rejection of the Bid.

6.6 Cost of Preparation

The Bidder shall bear all costs associated with the preparation and submission of its Bid and the Bank will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the Bidding process.

6.7 Normalization of Bids

The Bank will go through a process of technical evaluation and normalization of the bids to the extent possible and feasible to ensure that Bidders are on the same technical ground. After the normalization process, if the Bank feels that any of the bids needs to be normalized and that such normalization has a bearing on the commercial bid; the Bank may at its discretion ask all the technically shortlisted Bidders to resubmit the technical and commercial bids once again for scrutiny. The Bank can repeat this normalization process at every stage of technical submission or till the Bank is satisfied. The Bidders agree that they have no reservation or objection to the normalization process and all the technically short-listed Bidders will, by responding to this 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.

6.8 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. Technical Bid – Mandatory both Online (on GEM Portal) and Offline(Physical Envelopes - HEAD OFFICE IT DEPARTMENT 2ND FLOOR,PLOT NO. 151, SECTOR 44 INSTITUTIONAL AREA, GURUGRAM -122003)
2. Commercial Bid – Only Online (on GEM Portal), **Hard copy of the bid should not contain any Commercial information.**

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.

Deputy General Manager
Punjab & Sind Bank
Second Floor
IT Department
Plot Number 151, Sector 44, Gurugram, 122003
E-mail: hoit.tenders@psb.co.in

Online and Hard Copy bid submission is mandatory. The hard copies of bids of only those bidders who submitted bid documents online will be accepted. The hard copies of documents submitted should be same as submitted online without any commercials. 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.

6.9 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 both online and in hardcopy. Failure to submit the bid through both modes shall render the bid ineligible for evaluation. Additionally, if the Bidder submits the online bid but fails to submit the hardcopy by the deadline specified in Section 1: Key Information, bank has all the right to disqualify the bidder.

6.10 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

6.11 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.
2. The same 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.
3. 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.
4. Non submission of EMD leads to rejection of Bid.
5. All MSEs having registration as per provisions of the Public Procurement Policy for Micro and Small Enterprises i.e. District Industries Centre (DIC) or Khadi and Village Industries Commission (KVIC) or Khadi and Industries Board (KVIB) or Coir Board or National Small Industries Commission (NSIC) or directorate of Handicrafts and Handlooms or Udyog Aadhaar Memorandum or any other body specified by Ministry of MSME and Start-ups (recognized by DIPP) are exempted from submission of Tender Fee and EMD only. Relevant certificates should be submitted by the bidder in this regard to avail of exemption. Bid Security Declaration should be submitted by eligible MSEs/Startups on Company's letter head with company seal and signature of the authorized person as per Annexure-4.
6. The EMD may be forfeited/ Bank Guarantee 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.
- 7. 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.

6.12 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 for 10% 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 Service Provider 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 Service Provider is unable to service the contract for whatever reason.

6.13 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.

6.14 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.

6.15 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.

6.16 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://eprocure.gov.in/> & <https://punjabandsind.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.

6.17 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.

6.18 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.co.in by last date of submission of queries as defined in Key-Information in this document. Any queries or requests for clarification received after the stipulated time shall not be entertained.

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

Only two authorized representatives of the bidders who have purchased the RFP will be allowed to attend the meeting.

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.

Non reply to any of the queries raised by the bidder during the pre-bid Meeting shall not be considered as acceptance of the query/issue by the Bank.

6.19 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.

6.20 Disqualification

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

6.21 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.

6.22 Project Execution

The entire project needs to be completed expeditiously. The Bank and the selected bidder/s shall nominate a Project Manager immediately on acceptance of the order, who shall be the single point of contact for the project. However, for escalation purposes, details of other persons shall also be given. The project manager nominated by the bidder/s should have prior experience in implementing a similar project and meet eligibility criteria as defined in RFP

6.23 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 in the process of upgrading its IT security infrastructure and intends to implement advanced IT security technologies, a Security Operations Centre (SOC) solution, and related applications to safeguard its information assets at the Data Centre in Mumbai, Disaster Recovery Site in Noida, Cloud Environment, and bank's branches

This RFP invites technically mature, scalable, and interoperable solutions that will enable the Bank to establish a multi-layered defence posture covering Perimeter Security, Network Security, Endpoint Security, Application Security, Data Security at centralized level.

- 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.

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. Information/Digital Right Management
2. Centralized key management solution
3. S-BOM & C-BOM
4. Database Activity Monitoring
5. Mobile SDK
6. Identity & Access Management Solution
7. Multi Factor Authentication
8. Privilege Identity Management
9. Information Technology, Government Risk and Compliance

The Bank's approach is aligned with global standards and best practices such as **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.

The bidder shall be required to deploy a Project Management team during the implementation phase to ensure effective coordination and oversight.

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 selected bidder(s) will be responsible for delivering and implementing these solutions along with their respective deployment models: -

A. Endpoint Security

Solution Name	Use Case	Deployment Model
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-Premise

B. Application Security

Solution Name	Use Case	Deployment Model
Centralised Key Management	To ensure centralized lifecycle management of cryptographic keys, supporting secure generation, rotation, archival, and revocation across enterprise systems.	On-Premise
S-BOM & C-BOM (Software and Code Bill of Materials)	To identify and track all third-party and open-source components within applications to assess vulnerabilities and ensure software supply chain integrity.	On-Premise

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-Premise
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-Premise

D. Management Layer 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-Premise
IT GRC (Governance, Risk & Compliance)	To establish a centralized framework for tracking IT risk, control implementation, audit readiness, and compliance with regulatory and cybersecurity mandates.	On-Premise
Multi-Factor Authenticator	To strengthen authentication processes by implementing layered identity verification (e.g., OTP, biometric, hardware token) beyond traditional passwords.	On-Premise
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-Premise

Bidder to provide full-fledged services including but not limited to design, supply, implementation, configuration, customization, integration, migration, monitor, manage, backup, documentation, training, warranty support, post warranty maintenance support, arrangement with OEM and any other activities related to or connected to the Information Technology / Cyber Security Solutions & services, devices, applications & technologies together at the Bank during the entire contract period.

The complete implementation including **requirement gathering, designing, installation, configuration and implementation of the solution till the Go-live** of respective solution is to be done by the OEMs.

Bidder has to arrange for OEM's resources, and the bidder will be responsible for all co-ordination with the OEM and for completion of the implementation, within the timelines.

At the end of the implementation, the bidder has to arrange for a Certificate from the OEM, certifying that the implementation has been done by OEM's Resources and the deployed solution meets all the technical/functional specification of the solution as sought in the RFP.

1. System Integrator/bidder – Supply IT Security technologies, integrate IT Security with source IT & Cyber systems, provide onsite L1, L2 & L3 human resources for the duration of the contract and manage the project as defined in the RFP
2. Respective solution OEM – Deploy, install, integrate their own solution with every other solution / technology deployed in the IT Security setup, deploy required resources, migration of data and logs from current Security Solutions to new IT Security.
3. The solutions, agents, and instances of the security tools—whether proposed by the bidder or provided by the Bank—deployed within the Bank's infrastructure shall be extended to the Bank's Virtual Private Cloud (VPC) environments, including both those proposed by the bidder and those already existing within the Bank's infrastructure. This extension ensures that the monitoring, security, and management capabilities are consistent across both on-premises and cloud-based resources. Example SIEM Log collector instance would be deployed on VPC as well to collect the VPC logs and send them to SIEM & SOC-Big Data Lake.

Bidder to ensure all the commissioning, Integration, migration, relocation, updates, Upgrades, Patching, de-commissioning, Enhancements, Troubleshooting, Analysis, Health Checks, Backups, Audits, Documentation, SOP's, Creation of Knowledge Articles at Onsite for proposed IT Security solutions.

Every technology deployed in the IT Security solutions should collaborate with every other technology in IT Security & cyber security solutions on the real-time basis without manual intervention to leverage strengths of each other for studied analytics, correlation, reporting incidents and maintain overall false positive alerts within the threshold.

Dynamic, intuitive, parameterized and customizable dashboards should empower personnel resources in the IT Security to take prudent decisions. Multi-dimensional, analytical, trend & pattern-based dashboards should be recommended by individual technology based on their own self-learning capability.

Bank's security solutions agents (as identified by the bank like Third Firewall, PIM, DAM, XDR, HIPS, WAF, SIEM Log Collector, CSPM, etc.) will also be deployed in the cloud to maintain a consistent security posture across both cloud and on-premises environments.

The proposed solution, tools and IT Infrastructure must be OEM-supported, production-grade and stable (GA release), and should be implemented by/under OEM-certified resource supervision.

The supporting/underlying software like OS, DB etc. should be OEM supported software and shall be part of overall IT (On-premises and Cloud) infrastructure provided.

7.1 RACI (Responsible, Accountable, Consulted, Informed)

S.No.	Activity	Bidder	OEM	Bank
1	Requirement Analysis	A,R	R	C,I
2	System Design	A,R	R	C,I
3	Development and Installation	A,R	R	C,I
4	Configuration, policy, rules, posture definition, re-definition, assessment etc.	A,R	A,R	C,I
5	Documentation	A,R	R	C,I
6	Testing	A,R	R	R,C,I
7	Deployment & Go-live	A,R	R	C,I
8	Facility Management	R,A	C	C,I
9	IT Security Operations	R,A	C	C,I
10	Business Continuity Management	R,A	C	C,I
11	Architecture assessment	A,R	R	C,I
12	Rectification of any Points raised during assessment & reviews	A,R	C,I	I
13	Impact Analysis and Change management	A,R	A,R	C,I
14	Problem Management, Incident management, Service Support	A	A,R	C,I
15	Business Continuity Management	A,R	A,R	C,I

Bank based on required will adopt the best suitable approach for respective business applications, Security solution provider is required to design the proposed solution capable of meeting both the approaches.

7.2 Functional Requirements

7.2.1 Endpoint Security

7.2.1.1. 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 right for the same, both within and outside the organization.

Features & modules:

1. The solution is capable of rights retaining regardless of where files are stored, transmitted, used, and archived. Capable of applying rights and policies on the document irrespective of mode of document sharing i.e. SFTP, shared via One -drive, MS Teams, Share point, G-Drive, Dropbox, copied to USB etc. and should be independent of the collaboration platforms.
2. The Solution is having integration capability with existing DLP (Data Loss Prevention) solution and able to apply Keyword based / File Classification based document protection.
3. The bidder shall only install or use cryptographic modules based on authoritative standards and reputable protocols (Please refer to the Customer's Cryptographic Key Management Guidelines). The Service Provider shall implement strong cryptography and end-to-end application layer encryption to protect end user's sensitive data in networks and storage. The Service Provider shall implement or support encryption during data transmission, delivery or couriered to external parties or other locations.
4. System security is password controlled (for operating system, database, application and terminal id) which complies with the Bank's security policy (e.g. minimum password length, no. of attempts for logout, recycling of passwords etc.).
5. Solutions must have audit log feature to detect any changes in the tool and same should be integrated with SIEM for real time alerts.

Architecture/Deployment model:

1. Understanding the environment in terms of application, network, server and Security appliances, LAN, WAN & Internet Links and segments, privileged users etc. to ensure creation of use cases related to targeted attacks and early breach detection.
2. Integration and co-ordination with SOC.
3. The bidder is required to undertake the migration of historical logs spanning a one-year duration from all existing solutions to new setup. This action is intended to enhance the security posture and to comply with the audit requirements.
4. The solution must follow a multi-tier architecture and support high availability and disaster recovery.
5. Solution must scale efficiently to handle increasing volumes of documents, users, and data while maintaining optimal performance.
6. The IRM/DRM solution must support the Bank's Data Governance Framework and integrate with its existing infrastructure including SIEM, ITSM, LDAP, PIM/PAM, and DLP.
7. The solution should be capable of integrating with the Bank's Existing ManageEngine health monitoring tool.

Bidder/OEM Responsibility:

1. The OEM shall supply all necessary software licenses, install, configure, and implement the DRM solution.
2. The OEM must ensure integration with the Bank's SIEM, SOC Big data Lake solution for centralized monitoring and threat analysis.

3. The OEM is responsible for training the IT team on solution usage, policy management, and incident handling.
4. The OEM must provide first, second, and third level support, including bug fixes, updates, and upgrades as required.
5. The OEM should assist in defining classification and access control rules as per the Bank's data protection framework.

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

7.2.2 Application Security

7.2.2.1 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 interception, 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.

Features & modules:

1. The System shall support Multi-tenancy using multiple domains, Clustering, High Availability and Backup.
2. Solution should support Multi Factor Authentication (MFA) for users accessing protected path on Windows Servers
3. The Key Manager should offer various encryption and data discovery tools to locate the PII data in databases, images etc. captured by the web portal application giving a single glass pane view for centralized management.
4. The Key Management solution must have KMIP support to enable the solution to store the encryption keys of solutions providing native encryption ensuring that even if the disk drives (physical or virtual) are stolen, the data stored within them remains protected against unauthorized access.
5. Solutions must have audit log feature to detect any changes in the tool and same should be integrated with SIEM for real time alerts.

Architecture/Deployment model:

1. Multi-tier deployment across UAT, Pre-Prod, Production, and DR environments with high availability and disaster recovery capability
2. The System shall support Multi-tenancy using multiple domains, Clustering, High Availability and Backup.
3. Segregated network zones with strict communication flow between layers (one layer up or down only)
4. Integration with core banking systems, middleware, certificate authorities, and cloud key vaults
5. Centralized web-based administration for unified policy enforcement and real-time monitoring
6. Scalable design to handle increased volume of keys, users, and encrypted assets
7. The solution should be capable of integrating with the Bank's Existing ManageEngine health monitoring tool.

Bidder/OEM Responsibility:

1. Assess existing decentralized key setups and propose an implementation plan for centralization
2. Arrange PCI-DSS and ISO 27001 certification and ensure renewal throughout contract duration
3. Ensure role-based access controls, patching, updates, upgrades, configuration changes, data extraction, and audit readiness are maintained continuously
4. Integration with the Bank's core banking systems, SSL/TLS platforms, hardware security modules (HSMs), certificate authorities, SIEM/SOC platforms, DLP, PIM, IAM tools, cloud/on-prem encryption modules, and application servers to enable secure and centralized management of encryption keys and digital certificates across all environments.

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

7.2.1.2. S-BOM & C-BOM

The bank plans to implement a Software Bill of Materials (SBOM) solution to gain visibility into all software components, including third-party and open-source libraries used across banking applications. This will help identify vulnerabilities, outdated packages, and licensing issues early in the development cycle, ensuring compliance with RBI's cybersecurity guidelines on secure software supply chains and asset inventory.

In addition, a Cryptographic Bill of Materials (CBOM) solution will be deployed to monitor the use of cryptographic algorithms, certificates, and protocols. It will help detect weak or non-compliant encryption methods and ensure alignment with RBI-approved standards. Together, SBOM and CBOM will enhance application security, regulatory compliance, and audit readiness.

Features & modules:

1. Solutions must have audit log feature to detect any changes in the tool and same should be integrated with SIEM for real time alerts.
2. The solution must offer a portfolio view that pans across the entire footprint of applications being tracked in the bank.
3. Solution should be able to detect open-source packages and report related vulnerabilities, outdated versions, and license compliance risk.

Architecture/Deployment model:

1. Solution must ensure centralized and automated generation and management of SBOM/CBOM for all deployed systems.
2. SBOM/CBOM should cover on-premise, virtual, containerized, and cloud-hosted components.
3. Bidder shall integrate the SBOM/CBOM output with the Bank's vulnerability management and SIEM systems.
4. SBOM/CBOM data should be securely stored and accessible for audit, compliance, and forensic analysis.
5. Reports must support export in industry standard formats such as SPDX, CycloneDX, and JSON/XML.
6. The solution should be capable of integrating with the Bank's Existing ManageEngine health monitoring tool.

Bidder/OEM Responsibility:

Bidder shall provide a detailed SBOM and CBOM for all supplied components, ensure regular updates post-patching or upgrades, maintain integration with security tools, validate completeness during UAT, and ensure continuous compliance with regulatory frameworks like RBI, CERT-In, PCI-DSS, and ISO 27001.

Key Deliverables:

1. SBOM report covering software versions, licenses, source, and dependencies.
2. CBOM report listing all hardware, firmware, ports, interfaces, and communication protocols.
3. Mapping of components to known vulnerabilities (CVE listing) with mitigation status.
4. Evidence of integration with SIEM/vulnerability management tools.
5. Audit-ready compliance documentation and update logs throughout the contract lifecycle.

7.2.3 Data Security

7.2.1.3. 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.

Features & modules:

1. The proposed DAM Solution should capture and analyze all database activities by application user, Database users and/or privileged user accounts, providing detailed audit trails that shows the “Who, What, When, Where, and How” of each database transaction.
2. The Proposed DAM Solution should support automatic updates to the signature database and based on global threat intelligence, ensuring complete protection against the latest threats.
3. In The proposed DAM solution, audit policy and security policy should be mutually exclusive. The solution should be capable of generating security alerts even if an audit policy is not assigned to a given DB.
4. The proposed Risk Analytics Solution must provide behaviour analytics algorithm to establish behavioural baseline and find deviations
5. Solutions must have audit log feature to detect any changes in the tool and same should be integrated with SIEM for real time alerts.
6. The proposed DAM solution should be in adherence to the guidelines provided in the RBI cyber security circular no RBI/2015-16/418 dated 2nd June 2016. Subsequent, RBI guidelines, advisories to

be complied. DAM solution should be complied with DPDPA (Digital Personal Data Protection Act) 2023 and RBI outsourcing guidelines compliance.

Architecture/Deployment model:

1. A centralized system should enable the Bank to monitor, manage, and configure all database activity through a unified interface. Centralized management should support automation of routine monitoring tasks, policy reuse, and quick drilldowns for analysis and incident response, ensuring efficient and streamlined operations.
2. The DAM solution should integrate seamlessly with existing security infrastructure such as SIEM tools, syslog servers, reporting platforms, and multi-factor authentication systems. This integration should require minimal configuration effort and enhance the overall threat detection, log correlation, and response capabilities of the Bank's security ecosystem.
3. Architecture should have multi-tier, distributed, high availability at DC and DR deployment.
4. The solution should be capable of integrating with the Bank's Existing ManageEngine health monitoring tool.

Bidder/OEM Responsibility:

1. OEM must supply and configure centralized DAM management console for database activity log analysis, policy/rule-base management, and reporting.
2. OEM should integrate the solution with Bank's SIEM solution, PIM, IDAM, GRC, Vulnerability Management tool and hardening Management, Active Directory etc. No extra cost is payable for such integrations.
3. The OEM must create and maintain an inventory of all databases and database users, providing a detailed report to the Bank for validation and ongoing management.
4. The OEM shall configure granular access control policies and rights management rules, aligning with the Bank's security policies and segregation of duties requirements.
5. The OEM must enable real-time monitoring, blocking of unauthorized access, and sensitive data discovery/masking, with policies tailored to the Bank's specific needs.

7.2.3.1.1 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

7.2.1.4. 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 Omni Channel mobile

application. 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.

Features & modules:

1. Detect manipulation of device time settings using system events and external time validation.
2. Prevent keylogging by blocking malicious keyboards and detecting unauthorized input capture.
3. Identify code injection attempts through runtime integrity checks and anti-tampering measures.
4. Enable the SDK to identify and block connections to Rogue Access Points (RAPs). Solutions must have audit log feature to detect any changes in the tool and same should be integrated with SIEM for real time alerts.

Architecture/Deployment model:

1. The Mobile SDK shall be embedded into the Bank's mobile application during the build process, enabling runtime protection and security monitoring without requiring a separate application or agent.
2. The SDK shall support both Android and iOS platforms and ensure minimal performance overhead to preserve a seamless end-user experience.
3. The Mobile SDK must be capable of sending risk events and threat telemetry in a secure manner to the Bank's central monitoring systems without exposing sensitive user information.
4. Solutions must have audit log feature to detect any changes in the tool and same should be integrated with SIEM for real time alerts.
5. The solution should be capable of integrating with the Bank's Existing ManageEngine health monitoring tool.

Bidder/OEM Responsibility:

1. The Bidder shall be responsible for providing the Mobile SDK library, related documentation, integration support, and version updates as required during the contract period.
2. The Bidder shall coordinate with the Bank's mobile application development team to ensure successful integration and validation of the SDK in the existing mobile application environment.
3. The Bidder shall ensure the Mobile SDK is securely integrated with the Bank's proposed SIEM and SOAR platforms for real-time alerting, threat visibility, and incident response enablement.

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.

7.2.4 Management Layer Security

7.2.4.1 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 existing 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.

Features & modules:

1. Solution must provide dashboard view for various level of users / department heads - Top Management View (Board) – Having Summarized view of various department (Can be explored to show the detailed information pertaining to the particular / all departments (individually)).
2. Department Heads (Various Business & IT Department Heads) – Having detailed information pertaining to a particular department. The department head can have access to information pertaining to their department only. However, being a common department head, the head may have access to the information pertaining to more than one department. Executive committee (complete and detailed dashboard of the organization). System Administrator (for the systems associated with this administrator)
3. Solution must integrate with Bank's security information & event management (SIEM) solutions
4. Solution must have the capability to recommend risk mitigation actions for high-risk users, such as activity monitoring, ad hoc certifications, or remediation of policy violations
5. Solutions must have audit log feature to detect any changes in the tool and same should be integrated with SIEM for real time alerts.

Architecture/Deployment model:

1. The solution architecture should support multi-domain and multi-directory environments, allowing scalable deployment across diverse infrastructure landscapes.
2. It should be capable of integrating with the Bank's existing MFA, SIEM, SOAR, and other security and IT operations tools with minimal customization.
3. The deployment model should ensure high availability and fault tolerance, with the ability to operate across both primary and disaster recovery (DR) environments.
4. The solution should be capable of integrating with the Bank's Existing ManageEngine health monitoring tool.

Bidder/OEM Responsibility:

1. The OEM must deploy and configure the IDAM solution with all required modules—Directory Services, SSO, Lifecycle Management, Identity Governance, and Access Certification.
2. The OEM shall ensure integration of the IDAM solution with the Bank's HRMS, ITSM, Microsoft Active Directory, Microsoft Exchange, SIEM, SOAR, and PAM tools.
3. The OEM should define and document user management integrations with databases during the SRS phase.
4. The OEM must enable secure, scalable identity federation across heterogeneous directory systems.
5. The OEM should install and integrate with all the existing bank's applications and new applications

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, PAM, SIEM, and SOAR tools
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

7.2.1.5. 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. Overall scope must ensure full coverage of 24*7*365 monitoring & management aspects of Two Factor Authentication system.

Features & modules:

1. The authentication agents must support the following platforms:
 - i. Microsoft Windows - 32 Bit Platforms
 - ii. Windows Server - 64 Bit Platforms
 - iii. Apache Web Server
 - iv. Internet Information Server

- v. Red Hat Enterprise Linux
 - vi. IBM AIX
 - vii. SUSE Linux
 - viii. Oracle Linux
 - ix. Epic Hyperdrive
 - x. Rocky Linux
 - xi. CentOS
2. Self Service portal must include the following functions:
- i. Authenticator Enrollment
 - ii. Request token
 - iii. Replace token
 - iv. Change/Set PIN
 - v. Resync token
 - vi. Clear Security Questions
 - vii. Test Authenticator
 - viii. Report Lost Authenticator & Active Directory Password change and reset.
3. Solutions must have audit log features to detect any changes in the tool and same should be integrated with SIEM for real time alerts.

Architecture/Deployment model:

1. The solution must be designed for seamless integration with the Bank's existing IT landscape and security solutions.
2. It should be IPv6 compatible and fully operational in IPv6 environments at no extra cost.
3. The architecture should be flexible and adaptable to future changes in the Bank's network topology or infrastructure.
4. The MFA must support integration with SIEM and PIM solutions for centralized visibility and control.
5. The architecture, inventory, logistics etc. with respect to the token-based solution shall be the responsibility of the bidder.
6. The solution should be capable of integrating with the Bank's Existing ManageEngine health monitoring tool.
7. Solution should be capable for integration with TACACS solution being used by the Bank.

Bidder/OEM Responsibility:

1. The bidder shall supply, install, and configure both hardware and software components of the MFA solution.
2. The bidder must ensure integration readiness with existing and potential future systems including SIEM, PIM, and Fraud Management solutions.
3. Any required modifications due to network architecture changes must be provided at no additional cost to the Bank.
4. The bidder must ensure IPv6 readiness and provide continuous support for integration, updates, and system enhancements.
5. The bidder shall provide technical assistance for application and URL-level integration with the MFA solution as required.

7.2.4.1.1 Key Deliverables:

1. Fully deployed and configured 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.

7.2.1.6. 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.

Existing PIM Details

Augmentation performed in December 2024, License valid till Nov 2026

S.No.	Augmentation Details	Qty
1	Dell Vx Rail E660F (2.8 GHz, 24 Cores, 64 GB RAM, 800GB SSD, 4x7.6TB SSD Drives)	8
2	VxRail Software License (As a part of VXRail HCI Solution)	8
3	Dell Ethernet TOR Switch	4
4	Dell Management Switch	2
5	Microsoft SQL Server 2022 Standard core- 2 cores license pack	16
6	MS Windows Server 2022 Standard- 2 core license pack	192
7	End User License to access clients using ARCOS portal---PIMEU0IN	300
8	Client Manager license for Windows, Unix, Databases, Web Applications & Network/ Security Devices. Seamless SSO and Access Control Capabilities including, Server Manager License which allows managing access controls and complete audit trails for all client manager licenses managed by the solution, Password Management License for managing privileged user ID passwords mapped with ARCON with 2 Years Support	2100
9	Red Hat Enterprise Linux Server License	2
10	Array Virtual Load Balancers	4

11	Backup License	1
----	----------------	---

Note: Bank is having total 500 User licenses and 2300 service licenses

Features & modules:

1. Proposed solution must provide self-managed vault without relying on external RDBMS for any data storage. All components of the solution must be commercial grade. Provide database OEM authorization letter validating distribution & use of commercial grade database.
2. Solution must support inbuilt proxy for supporting secure session management across distributed environments. This functionality should not rely on native insecure tunneling of unix /linux OS or freeware utilities.
3. Solution must provide automatic execution and management of privileged tasks with prepackaged commands for easy automation of routine backup jobs, routine file movement activities, service execution based on application job schedules, data gathering from multiple systems, configuration checks & configuration change based on SSH, telnet and PowerShell interfaces.
4. Solution allows dynamic discovery and automatic onboard of cloud-based infrastructure
5. Solutions must have audit log feature to detect any changes in the tool and same should be integrated with SIEM for real time alerts.

Architecture/Deployment model:

1. Upgrade/replace of existing PIM Solution by deployment on new setup along with migration of existing data & information already integrated and working in the Bank's environment.
2. The PIM solution architecture should be able to consume existing PIM logs which enable the Bank to view and analyze existing logs and session recordings.
3. The PIM solution should support seamless integration with the Bank's SIEM, Network Access Control (NAC), ITSM tools, Identity and Access Management (IDAM), LDAP/Active Directory, Database Activity Monitoring (DAM), Vulnerability Management tools, and other existing or future security and IT infrastructure components as required by the Bank
4. The solution should be scalable to accommodate future growth in privileged accounts and managed systems.
5. The proposed solution should support API-based integration with existing and future IT and security solutions (on-premises/cloud) including but not limited to Active Directory, DLP, PIM, NAC, DAM, SIEM, NTP, Internet Proxy, and Ticketing tools.
6. Architecture should have multi-tier, distributed, high availability (DC and DR) deployment.
7. The solution should be capable of integrating with the Bank's Existing ManageEngine health monitoring tool.

Bidder/OEM Responsibility:

1. OEM must ensure that all the features available in the deployed version are implemented and resources are trained accordingly.
2. The OEM would integrate the solution with Bank's SIEM solution, DAM, Vulnerability Management tool, hardening Management, AD/LDAP, etc. with no extra cost for such integrations.
3. Integration of new servers regardless of OS/DB with new PIM setup on an ongoing basis.

4. OEM shall ensure compliance with DPDP, RBI outsourcing guidelines, and other regulatory requirements.
5. OEM shall provide knowledge transfer and training to the Bank's security team on managing and operating the PIM solution.
6. Bidder should integrate the proposed PIM solution to monitor network devices, servers, Web applications, databases, middle wares without dropping any log.

7.2.4.1.2 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

7.2.1.7. ITGRC

The Bank intends to implement a robust IT Governance, Risk, and Compliance (ITGRC) solution to establish a centralized framework for managing IT-related risks, ensuring regulatory compliance, and enforcing governance policies across all business units. The solution should enable systematic identification, assessment, and mitigation of risks while ensuring alignment with industry standards and regulatory requirements such as RBI guidelines, ISO 27001, and PCI-DSS. It should support key functionalities including risk management, policy and procedure management, control definition, compliance tracking, and audit management.

The ITGRC solution must offer automation capabilities for workflow management, real-time dashboards, alerts, role-based access, and integration with the Bank's existing IT systems such as core banking, cybersecurity platforms, access management, and incident response tools. This will allow the Bank to achieve continuous monitoring, proactive risk mitigation, improved audit readiness, and enhanced accountability through transparent and auditable processes. The goal is to create an enterprise-wide risk-aware culture supported by efficient, scalable, and compliant IT governance mechanisms.

Bidder to provide the rate card for the solution as per the format given in commercial BOM\

The proposed IT security Governance, Risk and compliance solution should be able to address the following key areas but not limited:

1. Drive more value from internal audit management activities
 - i. Streamline basic audit processes with intuitive documentation

- ii. Increase audit efficiency with better planning and reporting
 - iii. Improve business alignment with audit processes integrated with fraud management, process control, and risk management activities
2. Effective, ongoing controls and compliance management. Focus resources on high impact processes, regulations, and risks to get continuous insight
3. Preserve and grow business value with enterprise risk management. Understand what influences risk levels, how risks impact value, and which responses are most suitable with enterprise risk management.
4. Include the following attributes: IT Security Risk Management, audit management, regulatory and compliance management, business continuity and 3rd Party risk management (or modules that cover the same subjects).
5. All sub-modules must be relatable; i.e. centrally stored regulations should be accessible from each module; audit findings should be accessible in compliance/ERM modules, etc.
6. Leverage Microsoft Office Products (particularly Word, Excel, and PowerPoint) to allow data and chart exports for external reporting needs and to allow current data to be migrated into GRC product to create baseline policy and procedures library as well as programmatic templates, etc.
7. Help corporate boards, audit committees, executives, and operating managers:
8. Align risk management with business value drivers
 - i. Gain insight into how risks occur
 - ii. Act on emerging risks and opportunities
9. Scalable (capable of implementing one module/service at a time and adding users as needed).
10. Bidder should integrate the proposed IT security GRC solution with the Bank's existing policies
11. Bidder needs to ensure all existing compliance requirements of the Bank and other Banking regulatory bodies are incorporated
12. Bidder is responsible for migration of all the data and policies from existing solution to the proposed solution.
13. The IT Governance, Risk and Compliance solution should provide actionable reports, such as but not limited to below mentioned reports:
 - i. Governance Reports - The IT GRC Solution should monitor adherence to organizational policies, track stakeholder engagement and satisfaction and measure the effectiveness of governance initiatives.
 - ii. Risk Management Reports - The IT GRC Solution should evaluate potential risks to the Bank, provides a centralized view of identified risks, their impact, and mitigation plans, monitor critical risk metrics and assess the effectiveness of risk mitigation strategies.
 - iii. Compliance Reports - The IT GRC Solution should track compliance with regulations and standards, manage audit findings and remediation actions, evaluate the effectiveness of internal controls, identify compliance gaps and remediation plans and assess the impact of new or modified regulations.
 - iv. Audit Reports – The IT GRC Solution should outline audit objectives and scope, document audit findings and recommendations and track progress on audit recommendations.

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

Respective OEM along with the bidder is required to inter-work, liaison with existing vendor for having a smooth migration from existing solutions to the bidder proposed application/infrastructure.

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 a IT Security setup in its Data Centre premises at DC & DR.

Bidder is required to migrate the following from existing solution to new platform (but not limited to):-

1. Telemetry data
2. Logs
3. Rules/configuration/policies
4. Existing customization
5. Parsers
6. Meta data

Bidder is required to perform the mapping, create parser rules and etc.

The above requirements and approach need to be followed for all IT Security solutions and other security solutions wherever applicable as proposed by the Bidder.

The Respective OEM along with the bidder will explain how and when it will implement the migration activities, describe how it will perform the migration of solution & Services from bank's current environment. The Respective OEM along with the bidder is required to submit the project plan ("Detailed Project Plan") indicating the tasks, timeframes, resources, and responsibilities associated with the Migration activities. Respective OEM along with the bidder has to develop a detailed Migration plan covering at least the following key areas:

1. Migration Schedules, Tasks and Activities
 - Migration activities
2. Resource Requirements
 - Software Resources
 - Hardware Resources
 - Facilities Personnel
 - Other Resources
3. Relationships to Bank's other Teams / Projects
4. Management Controls
5. Reporting Procedures
6. Risks and Contingencies- Key Risks, issues, dependencies and mitigation plans.
7. Transition Team Information
8. Transition Impact Statement
9. Review Process
10. Configuration Control
11. Plan Approval
12. Describe tools, methodologies and capabilities of the teams deployed for transition.

Respective OEM along with the bidder is required to ensure that their framework for migration of proposed solution, services, data, logs etc. from Banks IT team/existing Service Provider at a minimum should include the following phases and allied activities:

Service Requirements	Description
Initiation	Kick off the Migration based on the agreed transition plan
Planning	This phase takes care of all the planning activities required for successful Migration of solution & services from banks existing vendor to the bidder
Execution	Execute the Migration of solutions & services while ensuring near zero risk and no disruption to business
Closure	Create all the documents and submit them to the banks for review and sign off and start off including the MIS & SLA reporting and maintenance of the in-scope applications & related infrastructure.

The Respective OEM along with the bidder shall be responsible for ensuring compliance with all implementation timelines.

In the event of any delay in the implementation of the proposed solution, irrespective of the cause, the Bidder shall be obligated to assume responsibility for the takeover and transition of all existing solutions and services currently implemented and operational within the Bank that fall within the scope of Bidder. The transition shall be executed from the Bank's existing vendor in a seamless and timely manner.

The Bidder shall deploy appropriate onsite personnel for the maintenance and management of the existing solutions. The number and qualifications of such personnel shall be commensurate with those currently deployed by the existing vendor, subject to approval by the Bank.

The Bidder shall be solely responsible for maintaining and managing the existing solutions and services until the successful go-live of the proposed solution. During this period, the Bidder shall ensure full compliance with the Service Level Agreements presently in force with the existing vendor.

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 the Bidder without recourse to the Bank.

Deployed manpower for maintenance & management of existing solution by the bidder shall be paid on actuals (Deployed & accepted by the bank) as per the rate (L1, L2, L3 & Project manager) quoted by the bidder in the Bill of Material in Year 1. The Bidder shall ensure the deployment of the aforesaid resources immediately upon any breach of the implementation timeline applicable to the respective solution.

7.4 Non-functional requirements

The important factors with respect to architectural requirements which bidder shall consider for implementation of the project are elaborated below:

1. The solution should be implemented as per best industry practices. It should be customized to meet bank's requirements.

2. Use of proven products and technologies - The proposed solution should necessarily consist of proven products and technologies for the required functionalities with any customization if required to meet the business objectives.
3. Scalability - All components of the solution must support scalability to provide continuous growth to meet the requirements and demands of BANK. The Solution should scale in a linear fashion and behave consistently with growth in data, number of concurrent users etc.
4. Interoperability - The solution should be interoperable, to support information flow and integration. It should support open architecture solutions such as XML, LDAP and SOA etc. where information/data can be ported to any system, whenever desired.
5. Availability - All components of the solution must provide adequate redundancy to ensure high availability. The solution shall have built in redundancy in terms of both the hardware and connectivity so that service is not impacted and is available 24x7.
6. Reliability – The solution needs to be reliable to maintain data integrity and support business continuity.
7. Security: Proposed solution should provide role-based security, encryption of data-at-rest, data in use, data-in-transit, and data on backup media.
8. The solution should be the latest version of proposed software with a clear product roadmap and should be in line with the current technology trends and business/domain trends. Bidder to note that proposed version of the solution should be latest stable & supported version from the OEMs and support from the OEM should be available for the entire contract duration.
9. Respective OEM along with the bidder shall comply with IS Policies, IT Policies, Data Governance policies and standards of BANK including data retention standard at all times.

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

The Respective OEM along with the bidder is required to comply with BANK IT, IS, Data policies etc. in key concern areas relevant to the RFP, details of which will be shared with the selected Bidder. Some of the key areas are as under:

1. Responsibilities for data protection, privacy, availability, and confidentiality.
2. Responsibilities for application security and availability.
3. Responsibilities on system and software access control and administration.
4. Custodial responsibilities for data, software, and other assets of BANK being managed by or assigned to the Bidder.
5. Physical Security of the facilities and access provided to the bidder professionals and other staff member.
6. Incident response and reporting procedures.
7. Password Policy of BANK.
8. Data Encryption/Protection requirements of BANK.
9. Bidder to ensure Data security for data in motion and at rest.
10. The Bidder shall provide extensive security features at the system and database levels to ensure security and integrity of the Data and the Application Modules.
11. Respective OEM along with the bidder to propose requisite tool to ensure encryption (Data at rest, data in transit/motion) and secure transmission of data. Bidder as a part of the technical proposal clearly indicate the security tools and solution proposed including the data encryption tools.

12. Respective OEM along with the bidder to ensure, configure and implement required tools/application to encrypt data at rest and encrypt data in transit.
13. Respective OEM and Bidder to ensure compliance to regulatory and statutory guidelines pertaining to information security, Data requirement and other applicable guidelines
14. All data—including but not limited to data used for storage, processing, license validation, telemetry, and logging—must reside strictly within the geographical boundaries of the Indian subcontinent. Under no circumstances shall any data or system component communicate with, transmit to, or be accessed from locations outside India. This includes preventing any form of direct or indirect connectivity, API calls, background services, or telemetry exchanges or any exchanges with external servers or regions beyond Indian borders.
15. To provide Forensic Investigation related information as and when required by BANK and share the required information/evidence with BANK
16. The Respective OEM is required to submit detailed security features supported by the system along with details and architecture of the security components.
17. The bidder shall share detailed information security incident report(s) with the detail of corrective actions taken if such a situation arises.
18. The Respective OEM along with the bidder should ensure that the Personally Identifiable Information (PII) is encrypted / masked, and all such PII should be masked accordingly in-line with access control mechanisms (for vendor teams including Support Engineers L1, L2, L3) as specified by BANK.
19. Security Configuration, Monitoring and Audit
 - i. The baseline security configuration of Operating System, Database, Web server and all other applications to be done by the Respective OEM along with the bidder, according to the industry best practices and same shall be shared with BANK for their review.
 - ii. Compliance with security best practices may be monitored by periodic security audits performed by or on behalf of BANK. The periodicity of these audits will be decided at the discretion of BANK. Periodicity for Regulatory Audits would be required as per the rules and guidelines laid down by the regulator or as required by the regulator. These audit plans include, but are not limited to, a review of access and authorization procedures, physical security controls, input/output controls, DB controls, backup and recovery procedures, network security controls and program change controls.
 - iii. To the extent that BANK deems it necessary to carry out a program of inspection and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of data, the Bidder shall afford BANK's representatives' access to the Bidder's facilities, installations, technical resources, operations, documentation, records, databases, and personnel.

7.6 IT Infrastructure requirements

1. Bidders must design, size, supply, commission, maintain and manage suitable and required hardware infrastructure for the proposed solutions in the RFP response at the location specified in the RFP (DC and DR). All the hardware/software should be replica at both DC and DR. Bidder should size hardware based on the volumes mentioned in Annexure 21: Volumetrics of this RFP at relevant locations- DC, DRC and branches.
2. If the proposed solution is cloud-based, the bidder must accurately right-size the cloud infrastructure to meet all performance, capacity, and SLA requirements outlined in the RFP. The design should ensure availability within the primary cloud site, incorporating failover, backups, and health monitoring, while also including a disaster recovery plan with a secondary site that meets the

defined requirement as stated in the RFP. The proposal should include detailed architecture diagrams and a sizing justification.

3. Bidder should arrive at the sizing independently along with the respective OEMs . In case, the sizing quoted by the Bidder fails to meet the necessary services, SLA and other terms of the RFP, bank will not bear any cost for upgrades or replacements. Also, during the contract period, growth of the bank should be considered and thus, the appliances, solution, IT Infrastructure proposed should have enough CPUs, memory, storage, NIC, Ports, etc. available to accommodate the predicted sizing, SLAs and other requirements of the bank as required. The appliance/devices/cloud environment proposed must have adequate vertical headroom. Any additional cost required for horizontal scaling would be borne by the Bidder in case of breach/ SLA bottleneck.
4. Bidder is required to propose a system which includes the OS, Database, compute nodes, storage system, network system, Backup Infrastructure & Solutions etc.
5. Bidder is required to provide staggered hardware, associated software and applications depending on the volumetric defined in the RFP. The warranty and subsequent AMC/ATS of the components will begin as per the phased delivery.
6. Bidder has to propose a dedicated non-production environment which can logically separate / Virtualized for Test, Development and Training. In case of on-premise solution, The bidder should note that the production and non-production environment should be physically separate to meet the requirement of the PSB.
7. Bidder is required to propose IT Infrastructure and applications for the following environments:
 - Production (DC and DRC)
 - Non-production (DC)
8. The non-production environments should have the same software and hardware setup as deployed in production environments meeting all RFP requirements.
9. All hardware (Production, Non-production, and related hardware components) and system software components required for the project, must be included in the bill of Material of the bidder. In case the bidder fails to do so, and the project demands additional components at a later stage, then the bidder will have to provide additional components at no additional cost to the bank. DB audit trails should be enabled across all environments and bidder is required to size the hardware accordingly.
10. Necessary services over and above this, such as implementation, management, SLA etc. will be the sole Responsibility of Bidder. The PSB expects Bidders to optimally size and factor the requirements in compliance with the RFP requirements. However, if at the time of implementation there is a shortfall/non-compliance of any component/hardware/software required for the functioning of Bidder's proposed solutions with respect to the proposed hardware/software, Bidder will be required to provide additional hardware/software at no additional cost to the PSB.
11. Bidder shall install and commission the required IT hardware assets and software components into the racks to build the required setup.
12. Bidder shall be responsible for providing all the logs and required telemetry data for the setup and ensuring its integration with the centralized SOC of PSB.
13. Bidder shall position a dedicated technical onsite team consisting of L1, L2 and L3 resources to implement, commission and manage the proposed set-up in managed services model in accordance with the necessary security policies and guidelines issued by GOI/MoD/MietY/Other regulatory & statutory body from time to time.
14. The bidder shall ensure that the SoPs, procedure, policies and guidelines etc. for the proposed infrastructure & solution must be fully compliant with the latest certification requirements of ISO

20000, ISO 27001, ISO 22301, ISO 27701, ISO 27017 etc. During the contract, if PSB/PSB appointed agencies identifies any shortcoming/ lack of compliance, the bidder shall be responsible to ensure compliance.

15. The bidder shall provision all the required hardware, software, licenses and other components required for the setting up of this management cluster and also ensure the availability of solutions as per the defined SLAs.
16. Entire solution (hardware & software) should be IPv6 implementation ready from day one, considering IPv6 security practices
17. Bidder to propose and factor the quantities required for any overhead for running the overall solution such as the orchestration, virtualization solution, containerization, or any other component as required.
18. Bidder can consider Logical separation/ Virtualization for production and non-production environment at compute and storage level for respective Environments. The bidder should note that the production and non-production environment should be physically separate with respect to Compute. Bidder is required to consider and propose SAN Switch, Backup Solution (Backup Software, Backup Server, Long term storage, D2D) which can be used both for production and non-production environment Logical separation / Virtualization / zoning.
19. Production Environment:
 - i. The virtualization should be implemented in such a way so that there is no single point of failure, in case of one instance / node is deployed in server 1 then the second instance / node of the same environment of the solution should not be deployed in the same physical server.
 - ii. Example: Assuming the proposed solution requires two web nodes say Web01 and Web02 and have three Production servers SRVPRD01, SRVPRD02 and SRVPRD03 with virtualization implemented; if Web01 node is deployed in SRVPRD01, then Web02 node is not allowed to be configured in SRVPRD01, it is to be configured either in SRVPRD02 or SRVPRD03.
 - iii. No two application instances will be deployed within the same rack.
 - iv. The Web Application can be virtualized to provide flexibility and scalability; however, it is important to note that the Web and Application tiers will reside in separate VLANs to enforce network segmentation and security. All east-west traffic between these VLANs will pass through a firewall to control and monitor inter-tier communication, ensuring strict access policies and reducing the attack surface. The architecture should be designed accordingly to support this layered security model.
 - v. The Database server will be deployed on a completely separate physical or virtual infrastructure, isolated from both the Web and Application layers, to further enhance security, performance, and fault isolation across the entire system.
20. Non-Production Environment:
 - i. The non-production environment must be physically separated from the production environment.
 - ii. The non-production Environment should be 15% of the DC- Primary in terms of Compute and Storage
21. Bidder shall provide legally valid Software/ hardware/ firmware Solution. The detailed information on license count and type of license shall also be provided to the Bank.
22. Bidder shall provide legally valid Software/ hardware/ firmware Solution. The detailed information on license count and type of license shall also be provided to the Bank.

23. The bidder is responsible to provide the correct sizing of compute, network, and storage, IOPS including server etc. in collaboration with the proposed OEM whose solution/technologies are proposed for IT Security for successful deployment. Bidder and OEM should also account for scalability and future growth of the Bank to arrive at sizing for the Contract period.
24. In the event of failure, the system should automatically initiate failover within seconds, ensuring uninterrupted functionality without requiring manual intervention.
25. All hardware and software components should be architected for seamless scalability at DC & DR, ensuring long-term capacity.
26. Each node/environment must be individually **provisioned for full peak load**

7.6.1 Compute Infrastructure

Bidders must design, size, supply, implement, maintain and manage suitable compute infrastructure for all the in-scope applications/solutions proposed in the RFP response.

The hardware sized should be redundant, both horizontally and vertically scalable, fault tolerant and designed for high availability.

Bidder has to provide the similar category (i.e., mainly same class - similar processor and OS platform) of servers for Test, Development and Training Environment as that of the proposed production.

Vertical and horizontal scalability should be two important requirements for the servers as well. Bidder should arrive at the sizing independently keeping growth roadmap in consideration.

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.

1. Proposed hardware should have separate FC/LAN Cards enabling separate subnet creation for backup process, if required.
2. The virtualization architecture must ensure no single point of failure. In case of one instance / node is deployed on server 1 then the second instance / node of the same environment of the solution should not be deployed in the same physical server.
3. The production and non-production environment should be physically separated to meet the requirement of the bank.
4. Production Environment:
 - Web and App can be virtualized/logically separated
 - Production - Database environment should be deployed on physically separate machines on different network subnets.
 - There will be separate virtual machines for Web Server, Application Server, and Database Server etc. All are in different logical zones separated through firewall to communicate with each other. Accordingly, the connectivity should be established to make them operational. In no case will communication be permitted without firewall and / or IPS. Bidder must ensure the communication in the desired way and all the required hardware, software and network equipment(s) etc., if required will be provided by bidder only.
5. Non-production:

- Bidder must propose a dedicated non-production environment which is logically separate / Virtualized for Test, Development, Training and other non-production environment etc.
 - These non-production environments should have the same software and hardware setup as deployed in production environments meeting all RFP requirements.
6. Necessary Hardware, Software and Services over and above this, such as implementation, SLA etc., will be the sole Responsibility of the Managed Service Provider/OEM. Managed Service Provider/OEMs to optimally size and factor the requirements in compliance with the RFP requirements. However, if at the time of implementation there is a shortfall/non-compliance of any component/hardware/software required for the functioning of the Managed Service Provider/OEM's proposed solutions with respect to the proposed hardware/software, Bidder will be required to provide additional hardware at no additional cost to the Bank.
7. Entire solution (hardware & software) should be IPv6 implementation ready from day one.

7.6.2 Storage Infrastructure – Primary & Object

Bidder will be responsible to design, size, supply implement and manage the Storage Solution in compliance with the RFP requirements at DC and DR.

Supply, installation and implementation of storage hardware (Primary and Object Storage), including SAN systems, with adequate capacity and IOPS (Input/Output Operations Per Second) as per requirements.

Bidder will be responsible for the comprehensive end to end design solution of the Storage across the sites which should include Minimal Data Loss, Replication and any other requirements stated in the RFP that relate to the storage.

Any component/software/service required by Bidder that does not fall under the existing Storage requirements must be factored by Bidder.

7.6.3 Backup Infrastructure

1. Bidder is required to size, design, supply, implement and manage the Backup Software along with necessary hardware (including backup storage) as part of the assignment.
2. Bidder to factor the required solution and infrastructure to ensure taking and securing backup as per the PSB policy (which will be updated from time to time). The sizing of the Backup solution has to be determined by Bidder in accordance with the storage sizing.
3. The bidder should configure, schedule and manage backups of all the data including but not limited to files, folders, images, system state, databases and enterprise applications as per the policy defined by PSB.
4. The scope of work also includes backup replication to DR Site.
5. Bidder must provide Backup solutions (on-prem solution with cloud ready capabilities) including required hardware, storage, software, and licenses for performing automated backups of configurations and data for IT Security solutions. The bidder should also ensure that sufficient storage is factored in during the contract period.
6. Backup & restoration solutions should be made by the team deployed by bidder aligning with the requirement mentioned in the Annexure 21: Sizing/Volumetrics
7. The bidder should be able to make the required modification in backup procedures as per PSB at no additional cost to PSB.

8. Additionally, in case any of the security application/tools is proposed on cloud, bidder is required to ensure the backup of proposed security solution on Cloud and provide the same to bank as and when required by bank.

Networking and Security Equipment:

1. Ensure network equipment is compatible with existing infrastructure and configured to optimize security, speed, and reliability.
2. Specify quality of service (QoS) settings, VLANs, and any necessary configuration protocols to ensure seamless data flow and security.

7.6.4 Software

Bidder should propose Enterprise/OEM Supported based licenses and must issued in the name of PSB. Only supported and stable version of solution can be considered for the proposed systems. The proposed solution should be the latest and stable version.

The bank will be entitled to use the new product features, upgrades, device models, new versions etc. without any additional cost to the bank.

Enhancement/ upgrades/ updates/fixes/patches/functionalities/subscriptions for hardware/ software/ Operating System / Middleware etc. should be implemented, post approval from bank, in the bank environment as and when released by Service Provider/ OEM or as per requirements of the Bank

7.7 Other requirements

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.

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.

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.

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

The OEM's must provide, maintain and update SBOM & CBOM as per CERT-IN guidelines including all the dependencies up to the last level.

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

1. The Respective Solution OEM along with the bidder must do in-depth study of all requirements and design and implement a solution taking them into account. The solution should be adaptive and responsive to requirements which may arise in future. The bidder's proposed solution must comply with the functional and technical requirements mentioned in RFP. But the bidder should not limit the requirements to this functional requirement list. As a part of the requirement gathering the OEM will conduct discovery and ideation sessions with BANK users and its appointed consultants to understand the requirements of the solution and the bank's existing infrastructure.
 - i. Respective solution OEM along with the bidder has to review the existing setup deployed in the Bank and provide best of design by factoring proposed supplied components and existing systems/components/devices which are in use.
 - ii. Respective solution OEM along with the bidder is responsible for formulating and recommending enterprise-wide security architecture of the Bank and security architecture for various applications deployed in the Bank.
 - iii. Respective solution OEM along with the bidder to study existing environment at bank, identify data sources required for integration, compliance, threat detection etc. and propose the solution architecture to the bank. The OEM needs to create a detailed reference architecture of the solution in consultation with PSB team.
 - iv. Few of the key activities includes but is not limited to the following:
 - a. Requirements elicitation with BANK 's team based on discussions, structured questionnaire, etc.
 - b. Leverage OOTB features/rules/parser/policies/controls etc.
 - c. Arriving at detailed requirements specification for the solution functionalities and exact data points
 - v. Respective solution OEM along with the bidder must coordinate with BANK 's vendor(s) of different applications & infrastructure to understand the data structure and field level mapping to extract the data/logs/installation of agents wherever required. BANK will only facilitate coordination.
 - vi. Systems Specifications Requirement Study: The Respective solution OEM along with the bidder will conduct a detailed requirement study to develop a Functional Requirement Specification Manual (FRSM) which would cover all the functions which would be offered to BANK. The functional requirements will also include all the functional requirements mentioned in Appendix 1A. Additionally, FRSM will also include functionalities which will be required by BANK in future. The FRSM will be handed to BANK for review and additions. All the additional suggestions given by BANK will be added to FRSM by the Respective solution OEM along with the bidder.
 - vii. Respective solution OEM along with the bidder will provide all functionalities mentioned in the Functional Requirement Specification Manual. Respective solution OEM along with the bidder will implement the proposed solution with all software, hardware, and infrastructure to meet functional requirements of FRSM.

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

1. The Respective solution OEM along with the bidder is expected to take up the role and drive overall solution development, customization, parameterization, and implementation of the proposed solution. The Respective solution OEM along with the bidder shall manage end-to-end service integrations and associated vendors.
2. Every technology deployed in the IT Security should collaborate with every other technology in IT Security on the real-time basis without manual intervention to leverage strengths of each other for studied analytics, correlation, reporting incidents and maintain overall false positive alerts within the threshold
3. The solution should enable to setup, configure, and customize the base solution for meeting the BANK's requirements
4. Respective solution OEM along with the bidder shall design the proposed system based on defined requirements, data flows and methodologies.
5. Respective solution OEM along with the bidder will be required to create:
 - a. High level system specification with overall architecture covering Technical Architecture including data flow architecture through the proposed systems.
 - b. Low level system specification with interface level details and elaboration of the High-Level Design (HLD).
 - c. The technical architecture should give complete details of the processes, interfaces, deployment, business including the flow of data from various sources to decision makers and the cleansing & transformation of data which happens in the process.
 - d. The Respective solution OEM along with the bidder shall create relevant documentations and seek sign off from BANK.
6. Respective solution OEM along with the bidder is required to study/ analyse, design a secured and dynamic architecture for the proposed solution.
7. Respective solution OEM along with the bidder shall be responsible for the overall Solution Delivery, Development, Installation and Configuration, and Vendor Management
8. The Respective solution OEM along with the bidder shall develop the system in scope, basis the design considerations along with exception handling, logging, archiving, monitoring, Definition of business rules to be implemented, writing deployment scripts, interface development, implementation of data exchanges, etc. Implementation of the Solution also includes all the Integrations as defined in scope and the unit testing of modules.
9. The Respective solution OEM along with the bidder shall design, size, implement, maintain & support the proposed solution on cloud.
10. The Respective solution OEM along with the bidder shall perform the role and take full responsibility for the end-to-end solution delivery. The Respective solution OEM along with the bidder shall design & deliver integrations between systems internal to BANK and external systems. The Respective solution OEM along with the bidder shall ensure flexibility to enrol third party / fintech companies / other bidders for data capturing / data validation / any other purpose and ensure the proposed solution integrates with BANK 's systems on a plug and play model.

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

1. Respective solution OEM along with the bidder to note that all development, installation, testing, Go-live activities have to be performed from bank's premise, no VPN/remote access shall be provided.
2. Respective solution OEM along with the bidder to note that Respective solution OEM along with the bidder is required to integrate the proposed solution & IT Infrastructure with ITSM & SLA Monitoring solution provided by bank.
3. Respective solution OEM along with the bidder should mandatorily ensure to collaborate with all necessary third parties & other OEMs. Any customization, enhancement and other device/solution administration related activity required in solution 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. without any extra charges to the Bank during the Contract period.
4. The Respective solution OEM along with the bidder should follow a suitable SDLC methodology waterfall/iterative/Agile/proprietary methodology, etc. as part of Bidder's response.
5. The new Security solutions proposed to be deployed under scope of this RFP, should be complete in all respects. There should not be any deployment dependency on any other third-party solution/licenses/ tools for implementation of proposed solution which is not factored from day 1. In case any such requirement of additional third-party solution/ licenses/ tools is there for implementation of proposed solution, the same should be clearly factored in the costing/ commercial details by the bidder under this RFP and the successful bidder must provide these third-party solutions/ licenses/ tools.
6. Deliver and implement the solutions & services to the Bank in compliance with International Standards such as ISO, PCI-DSS, etc. and advisories issued from regulatory authorities and statutory directions.
7. Any customization, removal of false positives, enhancement and other device/solution administration related activity required in solution 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. without any extra charges to the Bank during the entire Contract period.
8. The methodology should address development, customization, Managed services, Facilities management services, and hardware/software installation/configuration services.
9. The implementation shall be compliant to the Government of India/regulatory/statutory guidelines on storage of PII, Aadhaar information's, DPDP etc. The information should be encrypted and masked at the required screen and functionality.
10. Each of the steps should detail the input, process, and output in each step.
11. The details of the usage of tools/templates must be given.
12. Deliverables and sign off process for each of the deliverables at various stages should be provided.
13. The Respective solution OEM along with the bidder should ensure all process templates as per their CMMI/Quality certification is adhered to and provide to capture and prevent risks and issues.
14. The implementation of the software includes:
 - i. Functional requirements specifications/SRS/Detailed requirement gathering study
 - ii. SIT, UAT and other testing.

- iii. Live cut-over
 - iv. Customization
 - v. Configuration
 - vi. Installation
 - vii. Implementation
 - viii. Integration & interfaces
15. Activities and functions to be undertaken for installation and implementation of the software should be as per the RFP.
16. The bidder shall ensure that their personnel are actively involved during the development and implementation phases to facilitate skill enhancement and knowledge transfer from the OEM development team.
17. The sizing and provision of the required IT Infrastructure must be as per the requirement mentioned in the RFP document.
18. If the sizing is found inadequate and causes any performance issues, then the Bidder must provision additional IT Infrastructure & solutions/services as necessary at no additional cost to BANK.
19. The Bank is in the process of transforming its IT & Nextgen SOCsecurity infrastructure. The Respective solution OEM along with the bidder must take into account the reintegration of the proposed security solution with both the existing security infrastructure and any new security solutions acquired through this RFP or other RFPs.

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

Following is the indicative list of documentation that the Respective solution OEM along with the bidder should prepare, take BANK sign-off and submit it as a deliverable:

1. Detailed project plan
2. The following documents should be delivered by the Respective solution OEM along with the bidder to the Bank for every component/software including third party component/software before solution becomes operational of the solution (as applicable) :
 - i. User manuals
 - ii. Installation manuals
 - iii. Operation manuals
 - iv. Technical manuals
 - v. Software and Hardware requirement specification
 - vi. Secured configuration documents and Hardening document for all Security systems/solutions.
 - vii. System/database administrative documents Debugging/diagnostics documents Test procedures etc.
 - viii. High Level architecture document and Low-level architecture document.
 - ix. Deployment plan document.
 - x. Change management methodology document.
 - xi. Problem management methodology document.
 - xii. User management guide.
 - xiii. Release notes.
 - xiv. Impact matrix.

3. Secured Configuration document (SCD)/ baseline Hardening document for systems/ solutions under scope need to be reviewed on quarterly basis and modified, if needed. The same should be maintained with version controls

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

1. The Respective solution OEM along with the bidder shall deploy the solution in production environment, provide hyper-care support and maintenance. The Respective solution OEM along with the bidder shall observe the user working patterns, provide support, training, and technical help, fix issues/bugs being discovered in this phase and guide the users for best practices
2. Creation of deployment plan and planning go-live
3. Implementation, installation and fine tuning
4. Migration and go-live
5. Testing and fixes
6. User training
7. Issue/bug fixing
8. Red Teaming (or Purple Teaming) will be conducted by the bank or bank's appointed partner's after UAT, but prior to Go-Live or as part of security hardening and validation phase which shall include:
 - i. Security Validation- VAPT & IS AUDIT
 - ii. Incident & identification of gaps/blind spots along with the criticalities
 - iii. Readiness assessments
 - iv. Recommendations for improvement
9. Performance testing (Bidder along with the respective OEMs) at the start of UAT- To ensure the system can handle expected (and peak) loads while maintaining acceptable response times, resource utilization, and overall stability under stress or high concurrency are required to perform the performance testing using the proposed performance testing tools and perform the following activities:
 - Test system behavior under normal and peak user loads
 - System behaves under extreme or breaking load
 - As a part of the testing following pointers are to be measured, but not limited,
 - a. Response Time (avg, min, max)
 - b. Throughput (MB/sec)
 - c. CPU / Memory / Disk I/O / Network usage
 - d. Error Rate
 - e. System Recovery Time (after overload)
 - Performance testing cycle activities to be performed by Bidder & respective solution OEMs

Phase	Activities
Planning	Define test objectives, workloads, SLAs, use cases
Test Design	Model real-world scenarios (e.g., login, API queries, log ingestion)
Environment Setup	Isolate or clone production-like test environment
Test Execution	Run with baseline load, scale gradually
Monitoring & Analysis	Collect metrics via monitoring tools, OS-level, and application logs

Phase	Activities
Tuning & Re-testing	Identify bottlenecks, apply optimizations, re-test as needed

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

1. BANK proposes to conduct “User Acceptance Testing” (UAT) for the Solution for the purpose of ensuring that all the functionalities requested for by BANK are available and are functioning accurately. The UAT would be carried out for the entire suite comprising of the proposed solution and other sub-solutions proposed by the Bidder.
2. The Respective solution OEM along with the bidder shall convey to BANK that all the implementation, customizations, that are required to “Go Live” are completed and the solution is ready for testing.
3. The test environment to be always made available to BANK, for the purpose of testing. The Bidder is expected to provide for the requisite test and development infrastructure including hardware, software, operating system, and database for all applications being offered by the bidder. BANK expects the bidder to set up the required solutions and provide connectivity to test servers to BANK for the purpose of testing. BANK shall not pay any additional amounts to the Bidder for the purpose of creating the test environment. The bidder must ensure that all requirements for the test environment like storage, compute environment, etc. for the applications are taken into account. BANK plans to use the testing environment throughout the period of the contract.
4. Any deviations/discrepancies/errors observed during the testing phase will be formally reported to the Bidder and the Bidder will have to resolve them immediately or within the UAT timelines and guidelines formulated between the Bidder and BANK. The resolution timelines will be completely aligned to the project timeline of this RFP.
5. The Respective solution OEM along with the bidder will be responsible for maintaining appropriate program change control and version control for all the modifications/ enhancements carried out during the implementation/testing phase.
6. The Respective solution OEM along with the bidder will be responsible for providing and updating system & user documentation as per the modifications.
7. The Respective solution OEM along with the bidder is required to bridge the security gaps after taking appropriate approvals and concurrence from BANK.
8. The Respective solution OEM along with the bidder to review the following at the frequency specified by BANK:
 - i. Policies and procedures
 - a) Review policy / procedures related to the technology function and environment.
 - ii. IT General Controls review
 - iii. Logical Access
 - a) Review of user management procedures at application, operating system and database levels
 - b) Review of privileged access rights granted to application and system administrators
 - c) Review of account and password policy controls
 - iv. Physical and environmental Access Controls
 - a) Review of the procedures implemented at DC/ server rooms

- b) Assess the critical assets for environmental management system
- v. Change management process and system documentation
 - a) Review the program change management with respect to policy and procedures.
 - b) Review the procedures for requesting, development, testing and implementing changes.
 - c) Review the process for monitoring program modifications.
 - d) Review segregation of duties.
- vi. Third party Management
 - a) Review the process for monitoring and reporting on the achievement of service level performance criteria.
 - b) Review service level agreements for the maintenance and upkeep of the systems.
- vii. Backup and recovery process
 - a) Review backup related policies and procedures and compliance thereof.
- viii. Incident Management
 - b) Review incident management related policies and procedures and compliance thereof.
- ix. Business continuity management
 - c) Review the business continuity management related policies and procedures and compliance thereof.
- x. Security Review
 - a) Security and controls review of operating systems, database and applications.
 - b) Policies and security review of firewall, servers, routers and desktops

7.7.6.1 Quality Assurance

The Respective solution OEM along with the bidder shall be responsible for testing the system and ensuring that the performance, stability, continuity, reliability, etc. remains intact. The Respective solution OEM along with the bidder shall prepare test cases and perform thorough testing. The test cases, testing automation scripts, root cause analysis, bug fixes, workarounds/ troubleshooting measures for non-fixable issues and other testing activities related to different types of testing (functional, system performance, load/stress, volume, UI, exception handling, compatibility, etc.) should be documented, signed off and shared with BANK. The Respective solution OEM along with the bidder shall also define and document the entry and exit criteria for SIT and UAT. It is the sole responsibility of the Respective solution OEM along with the bidder to fix all the discovered issues during the testing performed. The indicative list of activities includes but is not limited to the following:

1. Test Preparation
 - i. Design Testing strategy for UT, SIT, load testing and as required by BANK
 - ii. Setting up of test environment which consists of IT infrastructure, software, and applications.
 - iii. Preparation of test data for all combinations to be tested
 - iv. Identification of test cases/scripts for which an automated script can be created, if applicable
 - v. Dry run test cases/scripts to verify that test cases are executing properly
 - vi. Finalize test plans / scripts / data
2. Test Execution

- i. Retest of failed test cases / scripts or modified scripts for testing the defect / deviation correction, if applicable
- ii. Recording, tracking, and reporting all defects/deviations, as well as resolving script and test defects.
- iii. Test results to be provided in an agreed-upon format that meets the standards and criteria specified by BANK
- iv. Final executed test scripts to be provided in a format that meets the standards specified by BANK
- v. Review and/or approval of the test results based on criteria defined in BANK standards for executed test scripts
- vi. Review and/or approval of the test results based on criteria defined in BANK standards for executed test scripts
- vii. Test summary report, including scanned copies of executed test scripts, consisting of screen prints and reports, in a format acceptable to BANK
- viii. Recommendations for the system, i.e., observations of system usability, suggested enhancements, and performance improvement

3. Unit Testing

- i. Unit testing of all the development, customizations, and configurations
- ii. Functional tests, Posture tests, Benchmark Comparisons, Operational tests, Load, Volume, Stress tests, GUI test, Compatibility tests, Exception Handling tests, Data Migration testing, Maintenance tests, Sanity tests, Installation test, Exploratory/Ad hoc tests and other applicable tests
- iii. Unit testing logs after the final modification to be submitted to BANK
- iv. Individual test cases developed after the final modifications have to be shared with BANK for necessary approvals & sign-off
- v. Documentations for workarounds and troubleshooting measures taken in case of non-fixable bug or issues
- vi. User usability testing – Usability testing allows Respective solution OEM along with the bidder to conduct user research with participants in their natural environment to test interaction and identity issue with navigation and layout.
- vii. Upon successful unit testing, the Respective solution OEM along with the bidder will proceed to SIT of the designed front end website.

7.7.6.2 System Integration testing

The Respective solution OEM along with the bidder should integrate the software with the Third-party agencies (Regulatory & statutory agencies, FINETCHs/ RegTechs/Feed Providers & partner Integrations) as per requirement of BANK and carry out thorough system integration testing. The vendor should also conduct the functional testing to verify that each function of the software application operates in conformance with the requirement specification.

System integration testing will be followed by user acceptance testing for all applications.

1. The Respective solution OEM along with the bidder shall test and ensure the performance, stability, reliability, request/response time, compatibility, etc. of all the interfaces between all the applications leveraged for the eco-system.
2. The Respective solution OEM along with the bidder shall fix all the discovered issues during the system testing and UAT phase related to the interfaces. The Respective solution OEM along with

- the bidder shall perform end-to-end system testing to ensure all the connected applications are appropriately operating.
3. The Respective solution OEM along with the bidder should integrate the software with the existing and proposed systems of BANK and 3rd party systems (as specified in Appendix 3)
 4. The system integration testing includes Interface/integration tests, Functional tests, Posture tests, Operational tests, Load, Volume, Stress tests, GUI test, Data Migration, Compatibility tests, Exception Handling tests, Maintenance tests, Sanity tests, Installation test, Exploratory/ADHOC tests, etc.
 5. All integrations of proposed solutions should be thoroughly tested.
 6. The Respective solution OEM along with the bidder is required to develop test cases, test scripts, provide test plans related to testing of all the interfaces between applications ecosystem.
 7. Set up and document all test data as described in the test scripts.
 8. Document steps for which integration of each component shall occur in the project's test plan.
 9. Perform integration testing iteratively with increasingly larger and more complex combinations of components.
 10. Verify the end-to-end process to work to confirm that fully integrated features behave according to specification.
 11. Perform negative testing.
 12. Document all test results, as well as any deviations that have been discovered.
 13. System integration testing will be followed by user acceptance testing (UAT), plan for which must be submitted by the Respective solution OEM along with the bidder to BANK.
 14. The Respective solution OEM along with the bidder shall perform Unit testing & System integration testing and submit their reports, findings, issues, etc. to BANK.

7.7.6.3 User Acceptance Testing (UAT)

1. The UAT includes functional tests, posture tests, operational tests etc.
2. The Respective solution OEM along with the bidder shall provide necessary information, tools and scripts to BANK users and their appointed consultants/vendors.
3. The Respective solution OEM along with the bidder will provide necessary on-site training for the purpose of enabling BANK and its appointed vendors.
4. The Respective solution OEM along with the bidder should carry out the load testing once the solution is deployed and submit the results to BANK.
5. If the testing results do not comply with BANK requirements, the Respective solution OEM along with the bidder shall provide and perform the necessary rectifications. The test scenarios should be created, reviewed and verified by Respective solution OEM along with the bidder and OEM and submitted to BANK for review.
6. Load testing shall be done in two round, Round 1 of load testing is to performed on the base solution before the start of UAT and round 2 should be performed on the UAT signoff solution (including the customization performed specifically for BANK). Any performance bottleneck has to be resolved.
7. The Respective solution OEM along with the bidder will set-up regression/automated test software and other tools which shall be used for BANK and the Respective solution OEM along with the bidder to implement-and operate the same.
8. The Respective solution OEM along with the bidder will prepare test cases, testing methodology and testing strategy for all the tests to be performed and submit to BANK for sign-off

9. The Respective solution OEM along with the bidder will create test data required by BANK to perform User Acceptance Testing (UAT)
10. Test plans, test cases, and test scripts for user acceptance testing to be provided by Respective solution OEM along with the bidder
11. Documentation of all test results, including any deviations that have been discovered in UAT by the Respective solution OEM along with the bidder
12. During the UAT testing, BANK will notify the Respective solution OEM along with the bidder at regular intervals the bugs/findings in writing
13. Respective solution OEM along with the bidder must fix these bugs, carry out necessary rectifications and deliver patches/version towards changes effected
14. BANK shall accept the application software only after the critical or major Bugs are fixed, which are then ready for production Implementation.
15. BANK may conduct reviews/audit, at its discretion, of the proposed solution and IT infrastructure during the contract period
16. The Respective solution OEM along with the bidder during the UAT stage shall submit the requirement traceability matrix and mapping of FRSM with the implemented solution

7.7.6.4 Data testing

Based on the stipulations of the RFP, the Respective solution OEM along with the bidder will be required to arrive at Test Methodology in consultation with BANK, based on a standard which is suitable for BANK.

Respective solution OEM along with the bidder will be responsible for performing the following activities for testing & Audits:

1. Development of suitable testing methodology/ testing strategy document
2. Development of test cases in consultation with BANK. The Respective solution OEM along with the bidder has to provide already prepared test cases to BANK (negative & Positive) which BANK may approve/ modify before execution.
3. Development of testing Schedule calendars.
4. Development of entry and exit criteria for testing.
5. Development of detailed test cases in UAT environment.
6. Train BANK's team in test cases development and testing methodology.
7. Test application software for functionality, operational convenience, security and controls. This will also include positive and negative cases for each type.
8. Execution of all the test cases.
9. Record test results against the test cases tested.
10. The testing should also ensure conformity to:
 - All customized menus and reports are working as per the SRS and BRD document provided by the Respective solution OEM along with the bidder.
 - All customized Interfaces are working as per the SRS and BRD document provided by the Respective solution OEM along with the bidder.
 - All functionalities are working properly as per the SRS and BRD document provided by the Respective solution OEM along with the bidder.
 - Gaps identified.
 - Interface testing with all types of transactions pertaining to that interface.
11. Point out gaps, errors, bugs during testing.

12. Document the gaps, errors and bugs observed during testing.
13. Maintain a track of errors, bugs and customization requests and their resolutions.
14. Explain bugs, errors and gaps to BANK and application vendors.
15. Follow up with Application vendor for fix or patch.
16. Re-test the gaps, errors and bugs after rectification.
17. Submit all documents on methodology, strategy, test cases, test documentation, customization requests, solution etc. to BANK.
18. Conduct unit testing, integration testing of the entire functionality of the solution.
19. All testing will be carried out with resources provided by the Respective solution OEM along with the bidder in coordination with BANK.
20. Respective solution OEM along with the bidder must fix the bugs, carry out necessary rectifications and deliver patches/version towards changes which would be reported by external agency and BANK.
21. BANK shall accept the application software only after critical or major Bugs are fixed and are ready for production Implementation.
22. Data Migration
Data integrity checks: Pre-migration and post-migration data sets should be compared for data integrity issues.
Data integrity checks should check the following data parameters:
 - i. Raw data integrity
 - ii. Business rules
 - iii. Log Tables
 - iv. Configuration/ Parameterization table

To ensure that the data in the newly migrated environment qualifies the integrity and reliability tests and in case any errors or mistakes are identified, suitable counter measures are taken by Migration team for mitigating their impact.

1. Identify the critical fields to be validated from the field in source system based on the experience of other migrations.
2. Business rules verification.
3. 100% of the Configuration/parameterization table should be verified.
4. Respective solution OEM along with the bidder is expected to verify log tables and highlight various error logs if any, post migration.
5. To provide an assurance that 100% data for critical fields has been properly identified and accurately and completely migrated to relevant data fields in the target system by understanding and validating the migration controls, performing independent verification of Data migrations
6. Review back-up procedure so as to ensure availability of data under conversion, the data is backed up before migration for future reference or any emergency that may arise out of data migration process.
7. Comparison of pre-migration and post-migration data for checking integrity issues.

Deliverables of data migration by Respective solution OEM along with the bidder

1. Data migration audit strategy.
2. Migration process review report
3. Field wise Exceptions reports (pre & post)
4. Data migration testing along with the scripts, testing status, risk categorization, impact etc.
5. Final compliance report, post migration.

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

Training & product certifications programs need to be arranged for PSB IT team without any additional cost. Upon completion of the training, the OEM shall issue certificates to all trainees.

All the technical product training should be provided by respective OEM. The bidder should submit a plan to the bank highlighting the baseline and levels of training and certifications required before deploying a person on the IT Security.

Training needs to be organized covering the following: new product features, workflows, changes made to the baseline set up of PSB IT Security, automation, best practices, advance security threats, market trends etc.

1. Beginner training by each OEM – Each Training session should be 2 Days Duration – Number of Training session should be 5
2. Advanced training by each OEM – Each Training session should be 3 Days Duration – Number of Training session should be 5
3. Backend system level training for troubleshooting, maintenance of systems – Each Training session should be 3 Days Duration – Number of Training session should be 5

7.8 ATS and AMC

Bidder should provide comprehensive **on-site** AMC for the remaining contract duration. The AMC for the hardware shall start with the installation & acceptance of the hardware by the bank.

Bidder should provide software licenses with comprehensive **on-site** ATS for the remaining contract duration. The ATS for the software shall start with UAT Signoff by the bank for the respective solution.

Rates provided by the bidder for the respective software, hardware and services shall be used on a pro-rata basis for any additional software, hardware and/or services utilized by the bank during the contract period.

ATS/AMC support must comply with the Technical Standards, Security Requirements, Operating Procedures and Recovery Procedures

If the bank buys any other supplemental hardware as agreed by the hardware OEM from a third party and installs it within these machines under intimation to the Bidder, then the OEM Support (ATS/AMC) should not become void. However, the ATS/AMC (Support from OEM) will not apply to such supplemental hardware items installed.

NOTE:

ATS-- Bidder to note that Total ATS/subscription cost for the respective solution should not be less than 75% of the Net License Cost of the respective solution

AMC -- Bidder to note that Total on-premises Hardware AMC Cost for the respective products should not be less than 25% of the Total on-premises Hardware Cost for respective items.

7.9 Resource Requirement

Key resources:

This is the minimum manpower requirement per shift. Bidder shall factor the total resource required to meet the below requirement.

Key Resources are PM – Implementation, Respective OEM Leads, PM-Operations, Any other proposed by bidder.

S.No.	Resource Type	Deployment	Count of Resources	Shifts (Minimum)	Experience/skillset
A) IMPLEMENTATION PHASE					
1	Project Manager – Implementation*	Onsite Full time	1	As per PSB timings and calendar.	<ul style="list-style-type: none"> B.E. /B. Tech /MCA/Any graduate At least one certification in Project management like PMP, Prince 2, etc. Minimum of 8 years of overall experience. Strong knowledge of Project management/Implementation management of Security solutions. The proposed resource should have experience of managing at least 2 solution (of which at least 1 perimeter security) Implementation in at least 1 PSU/ PSE/ Govt Department/ BFSI organizations/Regulatory Bodies of India.
2	Respective Solution OEM Resources	Onsite Full time	<Bidder/OEM to right size>	As per PSB timings and calendar.	At the beginning of the Implementation Phase before the start of requirement gathering phase, the OEM must submit details of the Onsite Resources (Resource deployment plan) assigned to each activity/milestone for the bank's approval. Any subsequent modifications or replacements aligned to each of the milestones will require the bank's approval.
3.	Bidder resources identified and tagged to each application/solutio	Onsite Full time	<Bidder/OEM to right size>	As per PSB timings and calendar.	At the beginning of the Implementation Phase before the start of requirement gathering phase, the bidder must submit details of the Onsite Resources (Resource deployment plan)

S.No.	Resource Type	Deployment	Count of Resources	Shifts (Minimum)	Experience/skillset
	n/services implementation				assigned to each solution activity/milestones for the bank's approval. Any subsequent modifications or replacements aligned to each of the milestones will require the bank's approval.
B) O&M PHASE					
1	L1 Resources	Onsite Full time	Please refer below table	24 x7 Shift	<ul style="list-style-type: none"> • B.E. /B. Tech /MCA/Any graduate • At least two certifications from recognized Cyber security OEMs or a recognized security certification such as CISA, CEH • Minimum of 2 years of overall experience. • Strong knowledge of IT Security Solution • The proposed resource should have experience of managing at least 1 IT Security solution (any solution in the same domain as for which the personnel is proposed) in at least 1 PSU/PSE/Govt Department/ BFSI organizations/Regulatory Bodies of India.
2	L2 Resources	Onsite Full time	Please refer below table	24 x7 Shift	<ul style="list-style-type: none"> • B.E. /B. Tech /MCA/Any graduate • At least one recognized security certification such as CISA, CISM, CISSP. • Minimum of 5 years of overall experience. • Strong knowledge of IT Security solutions. • The proposed resource should have experience of managing at least 1 IT Security solution (any solution in the same domain as for which the personnel is proposed) in at least 2 PSU/PSE/Govt Department/ BFSI organizations/Regulatory Bodies of India. • The personnel proposed as L2 for DAM/IDAM should have relevant Certification pertaining to DAM/IDAM Solution

S.No.	Resource Type	Deployment	Count of Resources	Shifts (Minimum)	Experience/skillset
3	L3 Resources	Onsite Full time	Bidder to right size	Bidder to right size	<ul style="list-style-type: none"> • B.E. /B. Tech /MCA/Any graduate • At least one certification in Security solutions and a recognized security certification such as CISA, CISM, CISSP, CCSA, CEH, CompTIA, GCIH, or GCIA • Minimum of 7 years of overall experience. • Strong knowledge of IT Security solution • The proposed resource should have experience of managing at least 1 IT Security solution (any solution in the same domain as for which the personnel is proposed) in at least 3 PSU/PSE/Govt Department/ BFSI organizations/Regulatory Bodies of India.
4	Project manager - Operations	Onsite Full time	1	General Shift	<ul style="list-style-type: none"> • B.E. /B. Tech /MCA/Any graduate • At least one certification in Project management like PMP, Prince 2, etc. • Minimum of 8 years of overall experience. • Strong knowledge of Project management/operations management of Security solutions. • The proposed resource should have experience of managing at least 2 IT Security solution Implementation/operations in at least 1 PSU/PSE/ Govt Department/ BFSI organizations/Regulatory Bodies of India.

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 require 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

S. No.	Security Solutions	L1 (Minimum resource count)	L2 (Minimum resource count)	L3 (Minimum resource count)
SOLUTIONS				
1	DRM (Digital Rights Management)	2	1	1
2	Centralized Key Management			
3	S-BOM & C-BOM (Software and Code Bill of Materials)			
4	DAM (Database Activity Monitoring)	1	2	
5	Mobile SDK (Software Development Kit)			
6	IDAM (Identity and Access Management)	1	3	
7	IT GRC (Governance, Risk & Compliance)			
8	Multi-Factor Authenticator			
9	PIM (Privileged Identity Management)			
10.	IT Infrastructure Management	1	1	

Each shift team should have one team lead/shift in-charge & L2.

Resources would be required to be positioned in IT Security office, DC, DR or any office as per the bank's requirement.

Note-

1. IT Solution will be 24x7x365 environment and personal resources should be able to work in shifts and flexible working hours to support the operations.
2. In case of replacement, the following transitioning and knowledge transfer period is to be adhered: Project Manager: 60 days, other key personnel: 45 days and other personnel: 30 days. Bidder needs to inform Bank in advance before initiating the transition or KT period.
3. The quantity of resources listed in the table above represents the minimum required for on-site deployment. Bidders must ensure that their on-site and off-site deployments are appropriately scaled while adhering to these minimum requirements.
4. The deployment of L1, L2, and L3 on-premises must be right-sized across shift by bidder ensuring 24x7 support. Bidder is required to optimize resource allocation to ensure that each shift maintains a minimum quantity of resources as indicated in the table above.
5. The Resources are named resources which shall be deployed on the project and change of resources is not permissible unless explicitly required and shall be as per SLAs and post approval from BANK.

6. In case of replacement, the following transitioning and knowledge transfer period is to be adhered:
Project Manager: 60 days, other key personnel: 45 days and other personnel: 30 days
7. Bidder must deploy competent resources for the team to perform necessary implementation, maintenance and support as per the requirements of BANK. Bidder must deploy adequate resources to ensure that the systems are implemented within timelines, are up & running and customer services are not impacted. To ensure that the SLAs are met, the Bidder if required will need to deploy additional resources during the contract period without any additional cost to BANK.
8. Bank reserves the right to interview all the personnel resources to be deployed on the project and reject if not found suitable for the project.
9. At a later stage also if any of the personnel resources are found unsuitable to perform duties or any of the personnel resources violates any of the Bank guidelines, Bank may seek removal of all such personnel resources.
10. Bank expects to build a strong team and there should be no single point of dependency on any one individual. Bank's services should always remain immune to any such dependencies.
11. Bidder is required to obtain permission from the Bank in writing before removing any of the personnel resources from the project.
12. During the Rollout and Critical stages of the project, bidder should ensure the availability of their senior management to ensure smooth coordination and alignment of team/resources
13. The responsibilities of PM are outlined below:
 - i. Lead implementation effort.
 - ii. Primarily accountable for successful implementation of the project across bank.
 - iii. Act to remove critical project bottlenecks.
 - iv. Identification of working team members, and team leads.
 - v. Single point of contact for Bank's senior management.
 - vi. Ensure implementation timelines are met to achieve desired result.
 - vii. Monitor Change management activities during implementation.
 - viii. Identify and implement best practices across the Bank.
 - ix. Co-ordinate with OEM/OEMs for successful implementation of solutions.
 - x. Periodic reporting to bank on the implementation status, issues/ challenges faced and how these are handled.

7.10 Facilities Management

Bidder should provide qualified and experienced resources to work during the contract period for (but not limited to):

1. Data administration
2. System Administration
3. IT Infrastructure administration
4. Extraction and development of reports
5. Support technical and functional queries.
6. A technical team, to solve logged issues within SLA period

This facilities management (FM) would have to play a critical role in on-going support. All Operation & maintenance resources will be screened by BANK authorities positioned on the project. Replacement of a resource under unavoidable circumstances needs to be intimated to BANK in advance and the replaced resource should be equally or more qualified and experienced with due handover & Knowledge Transfer.

The Bidder is required to provide support and applicable patches as and when released during the contract period. Any observation raised by Regulators/BANK/Other Agencies from time to time should be rectified and fixed by the bidder at no additional cost to BANK post approval from BANK for deploying the same Support & Maintenance.

7.10.1 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 on-site, by the OEM every year 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:
 - i. Diagnostics for identification of product or specified software failures and Root Cause Analysis (RCA)
 - ii. Protection of data/ configuration
 - iii. Recovery/ restart facility
 - iv. Backup of product or specified software / configuration
 - v. 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:
 - i. Overall maintenance and working of the solution.
 - ii. Bug fixing and delivery of patches/ version changes effected
 - iii. 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.
 - iv. 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:
 - i. All deliveries (full or patch) shall include a release note containing a full list of the contents of the delivery:
 - ii. Versions, file sizes and file modification dates of all components included in the delivery
 - iii. 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
 - iv. 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
 - v. 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. IT Infrastructure Operations includes but not limited to:
 - i. Major Incident Management
 - ii. Determining scope of the problem
 - iii. Managing the incident through service restoration
 - iv. Validating severity classification of the problem
 - v. Facilitating Service Recovery Team meeting
 - vi. Escalating the issue as required
 - vii. Conducting Root Cause Analysis
 - viii. Preparing restoration plans
30. IT Infrastructure Operations – System Operations includes but not limited to:
 - i. Monitor Cloud infrastructure
 - ii. Administer and/or execute Service processes and procedures
 - iii. Perform problem determination on systems and components managed by Bidder which include:
 - a. IT Infrastructure, System Software and Network problems
 - b. Evaluate planned changes to IT Infrastructure environment and advise requirements to support such changes
 - c. Monitor status of system processes
 - d. Monitor and respond to system/hardware alerts and events, application alerts and application file system space issues
 - e. Monitor and maintain system error logs
 - f. Perform required batch setup activities (ad hoc requests)
31. Compute Planning includes but not limited to
 - i. Configuration Management
 - ii. Performance Management
 - iii. Capacity Management
32. Storage Infrastructure Installation and Maintenance includes but is not limited to
 - i. File Management

- ii. Management of non-root application file systems including modifying file system sizes
- iii. Storage Environment Management including SAN Switch and device configurations Management, and disk storage arrays and tape libraries configuration
- 33. Monitor hardware and system software status, process status, and take necessary action based on detected problems or issues.
- 34. Provide problem escalation and interact as necessary with third party suppliers.
- 35. Provide monitoring and troubleshooting for the entire in-scope IT infrastructure.
- 36. 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.
- 37. Monitor the status of system processes and events.
- 38. Monitor and respond to hardware, system alerts and event.
- 39. Monitor and maintain system error logs.
- 40. Perform application, database, storage replication across the DC & DR as per required Service Levels.
- 41. Shifting of IT hardware within the premises, reinstallation and configurations including cabling and asset labelling.
- 42. Execute 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.

7.10.2 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.

7.10.3 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 License, 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. L3 personnel resources are expected to provide guidance to L1 & L2 resources. These resources must understand daily activities of L1 & L2 resources and automate the same in phases to achieve automation by the end of first year of operationalizing IT SECURITY setup.
7. Participate and contribute to every DR drill, cyber security drill, table-top exercises by the Bank, regulators or any third party.
8. Conduct DR drill of the IT SECURITY on quarterly interval or as and when required by the Bank.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. Creating new reports and customize existing reports, dashboards, rules, queries, user interface in all forms to meet the dynamic requirements of the Bank.
15. 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.
16. 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.
17. 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.
18. 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.
19. 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.

20. 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.
21. 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.
22. 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.
23. 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.
24. 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.
25. The IT SECURITY setup must be complete in all the respect with different solution components of IT Security and SOC are fully integrated to deliver the functionality as one comprehensive solution to ensure logs are captured and the process is automated to perform the desired processes in real-time basis 24x7x365. The system should also be automated to raise the alert to the designated official(s) of the Bank, if there is no log received for a period of 15 minutes. This duration of 15 minutes would be reviewed and reduced depending on the future requirements of the Bank.
26. Review onsite & offsite users as per Segregation of Duties (SoD) like their roles & responsibilities, access level / rights in the IT SECURITY 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.
27. The digital forensic investigation should be conducted as and when required capturing the complete replay of attack including the ingress and egress of payload in order to provide the exhaustive insight and findings on "Who did it, what did happen, when did it happen, where did it happen, how did it happen, whom did it impact" for each security incident. This entire process should be fully automated with tight integration and collaboration among all the components of deployed IT SECURITY solution.
28. Monitor, detect, prevent and appropriately respond against any known and un-knowns security threat, risk, bots' identification etc.
29. Bidder must provide the summary & presentation before going for any major hardware/firmware/middleware/software version upgrade to cover all new functionalities, features and bug fixes that are coming with new version/upgrade.
30. During the entire Contract period at any point of time, if the performance of any system of IT SECURITY setup is found to be not satisfactory as per RFP requirement then the Bidder shall be responsible to upgrade the hardware, software, applications etc. to meet the RFP terms at no extra cost to the Bank.

31. Bidder to ensure that the IT SECURITY technologies/solutions, services are capable & configurable to send logs, data, network traffic, security alerts etc. on demand to regulators like CERT-in, NCIIPC, RBI etc.
32. If any hardware, software, application, services has got additional component, feature, functionality, load bearing capability, domestic & foreign compliance requirements, security arrangement etc. the same can be activated or provided to the IT SECURITY setup just by activating licenses and without procuring any hardware, then the same should be activated and provided in the IT SECURITY setup of the Bank without any extra cost to the bank.
33. Email and Telephonic Support should also be provided by the back-end experts to the On-site support team.
34. 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.

35. Application management includes but not limited to:

Task	Activities
Services required	<ol style="list-style-type: none"> 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 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)

Task	Activities
	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.

36. OS/Server/Appliance/Hardware Management categorized under Incident, Problem and performance Management Services

37. Bidder needs to provide below mentioned services but should not limit itself to this list:

- i. Account administration
- ii. Performance, Incident and Problem Management
- iii. Monthly / Fortnightly call analysis
- iv. Device rights control
- v. Monitoring service availability, resource usage i.e., CPU, memory, disk space usage, storage bandwidth and utilization, load balancing, service performance,
- vi. Preparation of Preventive Maintenance calendar, Checklist, Root cause analysis and Capacity report
- vii. Updating knowledge base, Service pack, patch, and Antivirus definition
- viii. OS Hardening
- ix. Troubleshooting system alerts with knowledge base
- x. Closure of new incidents
- xi. Primary site /Secondary site failure testing along with BANK where the operations will be carried out from secondary site.
- xii. Liaise with Vendors for escalation.
- xiii. Audit of administrator accounts and log file archives
- xiv. Testing of backup tapes for data reliability, patches, and service packs
- xv. Patch Implementation
- xvi. Network reachability
- xvii. Configuring backup jobs
- xviii. Log analysis and monitoring
- xix. Rotation of Log file
- xx. Restoration Drill
- xxi. Defining Backup Policy, adherence to backup schedule and troubleshooting backup failures
- xxii. Performance Tuning

38. System administration services

Task	Activities
Client account maintenance	1. Creating users, groups, user accounts 2. Disabling user accounts 3. Modifying user accounts, etc. on the system 4. Review and approval processes

Task	Activities
File / system / access management	<ol style="list-style-type: none"> 1. Maintaining file and directory permissions on OS 2. Application access management like creating user accounts at application level 3. Access management should be adaptive, based on browser, location, device, time, holidays, etc. 4. Assigning application access 5. Setting application passwords, user lockout, etc.
Security monitoring and investigation	<ol style="list-style-type: none"> 1. Monitor physical security 2. Assess risks on a particular system OS environment and user needs 3. Monitor network security 4. Monitor denial of service attacks, bad bugs programmed threats etc. 5. Track logins, logouts, command runs 6. Perform regular security audits, etc.
Performance optimization and reporting	<ol style="list-style-type: none"> 1. Process and Memory Management 2. Monitoring CPU performance 3. Monitoring Memory performance 4. Conduct root cause analysis 5. Monitoring Input / Output performance 6. Monitoring Internet and Ethernet Traffic 7. Monitoring Load balancing 8. Monitoring Storage Bandwidth 9. Error detection and correction 10. Troubleshooting and client support, etc.
Backup File Retention	<ol style="list-style-type: none"> 1. Creating backup schedule 2. Performing backups and restoring files 3. Storing backups, Bidder should take backups for the entire period of contract.

39. IT Service Desk and Managed Services

Service Desk and Managed Services Levels:

- Level 1 Service desk
- Level 2 Service desk
- Level 3 Service desk

Level 1 (L1) Support:

- Role of L1:
 - Serve as IT Service desk front-end for all users
 - Provide services request sorting and ticket routing, if not applicable to bidder
- Problems that L1 would address.
 - Business application related issues/queries
 - Queries related to business process, reports generation, presentation layer applications, etc.
 - Enterprise applications (In-Scope), Operating System, Database, Middleware, Application server software, Generic IT Queries, IT Infrastructure queries
 - Other environmental software related to the proposed solution
- L1 staff responsibility
 - Assessment in case of specific rights assignment
 - Provision for assigning user rights only for certain fixed period

- iii Creation or modification of user profiles
- iv Periodic user right monitoring (at known frequency) must be specified and implemented
- v Categorization of requests into functional clarification, bug or change request
- vi Functional clarification/ workaround to be provided by Level 1 support itself
- vii Logging bug and reporting for further processing
- viii Provide support through telephonic and/ or electronic mechanisms for problem reporting requests and for service and status updates

Level 2 (L2) Support:

- a. Role of L2:
 - i. Should cover entire management and support of the proposed solutions and all third-party solutions
 - ii. To act upon the tickets routed from Level 1 (L1)
 - iii. To address issues/queries related to the applications, i.e., proposed solutions and all proposed infrastructure
 - iv. To assess cause of the issue and accordingly resolve the same within the timelines
 - v. Track problems from initial call to restore to service
- b. L2 staff's responsibility (Bidder needs to provide mentioned services but should not limit itself to this list)
 - i Troubleshoot any query processing, online processing, or batch processing activity at various levels in the proposed solution
 - ii Resolve the call within stipulated timeframe as defined in SLA by coordinating with the L1 or L3 teams if required
 - iii Escalate unresolved calls as per escalation matrix
 - iv Automatically log in calls during escalation
 - v Provide the timeframe for providing a resolution of the escalated calls
 - vi Decide on preventive maintenance schedule with BANK
 - vii Prepare a root cause analysis document with the resolutions provided for major issues such as: Production issues, Problems resulting in complete service disruptions or downtime, Delayed response times, Data /table corruptions, System Performance issues (high utilization levels), etc.
 - viii Application database and presentation layer support
 - ix Support and maintain all interfaces to the proposed solution and other solutions part of this scope document
 - x Modifications to existing scripts, reports
 - xi Present to BANK management on critical issues reported, resolved, solution provided and suggested recommendations or leading practices as and when asked by BANK or monthly, whichever is earlier
 - xii Perform performance tuning of the applications including database tuning
 - xiii Rectify any corruption in the software
 - xiv Ensure patch releases are deployed to the production environment with no business disruption or business loss
 - xv Support BCP/DR drills
 - xvi Provide application support
 - xvii Routing the transactions through the backup system in case the primary system fails
 - xviii Providing BANK with hardware utilization reports (as per the frequency directed by BANK) and alerting in case of any performance issues or hardware upgrade requirements
 - xix Support for integrating any applications that need to be interfaced with the proposed solution in the future

- xx The engineers are expected to provide following services: Configuration changes, version up-gradations, performance monitoring, trouble shooting, patch installation, running of batch processes, database tuning, and liaison with respective product owner/OEMs and/or CSP for various support issues, taking periodic backup of the database, query generation, etc.

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

Level 3 (L3) Support:

- a. Role of L3
 - i To handle all critical code level changes or issues related to hardware failure
 - ii The support is required for all components that are mentioned in this RFP
- b. L3 staff's responsibility (Bidder needs to provide mentioned services but should not limit itself to this list)
 - i Resolve the call within the stipulated timeframe as defined under the SLA
 - ii Updating status, resolution or workaround and date of resolution and informing BANK on the same
 - iii Preparing a root cause analysis document for issues referred to L3 support and provide to BANK along with the resolution
 - iv Liaise with L2 support personnel for the call information and resolution
 - v Provide version upgrades and
 - a. Perform version migration as per the version release plan of product owner/ OEM and agreed by BANK. It also includes porting of existing customizations
 - b. Provide training to BANK's core functional and technical team members on the new version functionalities and technical aspects
 - c. Plan and schedule implementation for the upgrades with BANK

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

7.10.4 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:
 - i. Identity and Access Management
 - ii. Privilege Identity Management
 - iii. Database Activity Monitoring
5. Incident Handling and OEM Involvement:
 - i. 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.
 - ii. 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.
 - iii. Regular collaboration with OEMs should also include proactive reviews, patch advisories, configuration validation, and support for root cause analysis, where applicable.

7.10.5 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 starting of the project and every MONTH highlighting the updates made in the document with respect to the previous version.
 - i. Disaster Recovery Plan- identifying the operations involved in disaster recovery and the dependencies between these operations.
 - ii. Disaster Recovery Procedures- providing step-by-step instructions for the operations identified in the Disaster Recovery Plan
 - iii. 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

7.11 Other In-Scope services

7.11.1 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 & Appendix 1B: Technical 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 Go-Live of the respective application (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 finalised 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 operationalise 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.

7.11.2 Escrow

The Bank and the Bidder shall agree to appoint an escrow agent to provide escrow mechanism for the deposit of the source code of any customization done on Commercial off the shelf software products supplied/ procured by the Bidder to the Bank in order to protect its interests in an eventual situation. The Bank and the Bidder shall enter into a tripartite escrow agreement with the designated escrow agent, which will set out, inter alia, the events of the release of the source code and the obligations of the escrow agent. Costs for the Escrow will be borne by the Bidder.

7.11.3 Exit Plan Management

1. The scope of work mentioned is illustrative and not exhaustive. Bidder needs to comply with the Bank's requirements and any statutory or regulatory guideline(s).
2. Bidder to provide Termination/Expiration Assistance regardless of the reason for termination or expiration
3. Bidder to comply/adhere to the Exit Plan
4. Bidder will not make any changes to the Services under the Agreement and continue to provide all Services to comply with the defined Service Levels.
5. Bidder to perform reverse transition of services to the bank's new vendor or bank's officials.
6. Bidder shall within ninety (90) days of the Signing Date, deliver to Bank a plan specifying the Termination/Expiration Assistance including functions and services of Bidder necessary to accomplish the transfer of responsibility of the Services from the Bidder to the Bank or a Third Party. In the event of Term Expiration or termination of this Agreement, the plan shall at minimum, contain Bidder's detailed plan for Operational and Knowledge Transfer requirements and list of documentations.
7. The Exit Plan shall be updated by the Bidder on an annual basis in accordance with Bank's requirements and delivered to Bank for its approval on or before the start of each Contract Year.
8. Knowledge Transfer and Handover of Services
9. Bidder to provide transfer of knowledge w.r.t. Services
10. Provide Bank's personnel or designated third party personnel training for the Services that are to be transferred.
11. Bidder shall train Bank's designated personnel and/or its designee(s) for any process or associated Equipment's, Materials, Systems or tools used in connection to the Services
12. Provide Bank and/or its designee(s) information regarding Services (as necessary) for implementation of the Exit Plan. Bidder to also provide information regarding Services as reasonably necessary to the Bank or its designee(s) to overtake responsibility for continued performance of Services in an orderly manner so as to minimize disruption in operations.
13. Provide Bank or its designee(s) a complete copy of the Bank's IP that are in Bidder's possession and Bidder's IP that Bank is licensed or otherwise authorized to use.
14. Explain the change management process, problem management process, Policies and Procedure Manual, reports and other standards and procedures to Bank's or its designated staff.
15. Provide technical documentation for Software used by the Service Provider for continued Services
16. Identify, record and provide release levels of Software and update of records of release levels prior to and/or during transition of Services
17. Provide assistance to the Bank or its designated officials for notifying the third-party vendors for procedures to be followed during the transition of Services.

18. Ensure transfer of Configuration Management Database (CMDB) that contains details of data elements that are used for management of Services. The CMDB must be in a form that can be migrated to a new environment that can manage Configured Items.
19. Bidder shall provide other technical and process related assistance, as requested by the Bank.
20. The bidder will not be allowed to take bank's IP information.
21. If the Reverse Transition is within the contract period, the successful bidder will be paid as per the support charges agreed in this contract, during the transition period till the completion of reverse transition. If the Reverse Transition occurs outside the contract period, then it will be mutually agreed terms and conditions. The transition out phase and the support required from the Successful Bidder shall be communicated to the Successful Bidder before the transition starts. The bank shall reserve the right to revise the transition period. During the Transition Period, successful bidder shall at least, but not limited to, provide support in terms of transition of assets and data, training and knowledge transfer and any other type of support during the defined transition period.
22. Bidder is required to provide the data dictionaries and data in the requested format to the bank/banks identified bidders.

7.11.4 Security Management

1. User id and login should determine level of access to data e.g. read/view data, print data, write/modify data, delete data etc.
2. The solution should support the following security features:
 - i. Username and password for accessing the applications and database
 - ii. Access credentials should not be stored on the endpoints
 - iii. Auto blocking/locking of applications access upon reaching maximum number of tries. The maximum number of incorrect errors should be defined by the Bank
3. Termination of session and log off after lapses of configurable time period.
4. The solution should support the following transaction level security:
 - i. End-to-End encryption of data transmission (symmetric or asymmetric)
 - ii. The solution should support multiple authentication-based bank's preferences
5. The solution should support the following platform security & reliability:
 - i. Data stored is encrypted in the platform database
 - ii. Audit trails and logging features must be available in Web Server, application server and database server
 - iii. Ability to assign specific rights to platform administrators for secure and restricted access
 - iv. Solution should have the ability to support external certifying authority
 - v. Solution should have secure interfaces to various hosts systems according to prevailing security standards
 - vi. Application access credentials should not be stored locally.
 - vii. Solution should support standard algorithms like AES
 - viii. 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)
 - ix. 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.
 - x. 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

- xi. OWASP Top 10 Compliant
- xii. Password must be hashed by SHA256 at least and include Salt or using salt supported cryptography
- xiii. 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
- xiv. Sensitive Data Exposure:
 - Sensitive data should be masked when output.
 - Sensitive data should not be stored in source code, config files and logs.
 - Passwords are hashed using Salt.
- xv. Configurable approval rules set up for Bank administrator to perform the actions
- xvi. Regulatory & Statuary
 - The solution should comply with the security principles and practices as stipulated by Statuary and regulatory authorities in India
- xvii. Application
 - OS Security check up. Application should have capability to detect if the application is running on a jail-broken / rooted / malware infected device.
 - Application must prevent hackers from accessing the application in a case where the device is rooted or jail broken.
 - Blacklisting/Blocking of older versions of the Application on the back end, if there is a security breach.
- xviii. Transaction Logs
 - Should maintain detailed transaction logs to enable processing audit trails to be reconstructed in the event of any disputes or errors
 - The storage and retention period of logs should be parameterized
 - Security safeguards should also be implemented to protect the information from unauthorized modification or destruction
 - System should facilitate maintaining logs.
 - Provision to generate detailed reports, logs, audit trails

7.11.5 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. During the extension period, the annual rates of respective support components shall not exceed 15-20% of the last year's support components (ATS/ AMC/ O&M/ Subscription/ Services) prices.

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 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 6 Months for all solution & services

A) Hardware & Software Delivery & Installations

S.No.	Activity/Milestone	Start date	End Date
1	Delivery of Hardware	T0	T1= T0+2 Month
2	Delivery of Software	T1	T2 = T1+0.5 Month
3	Installation of hardware	T2	T3 = T1 + 0.5 Month
4	Installation of software	T3	T4=T2+0.5 Month

B) Product Implementation Timelines: The timelines are applicable to each of the proposed products

S.No.	Activity/Milestone	Start date	End Date
1	Milestone 1: SRS, HLD, LLD Signoff of Respective application	T0	T1= T0+2.5 Month

S.No.	Activity/Milestone	Start date	End Date
2	Milestone 2: Implementation, Configuration, UT & SIT	T1	T2 = T1+2.5 Month
3	Milestone 3: UAT & UAT Signoff	T2	T3 = T2 + 0.5 Month
4	Milestone 4: Go-live preparedness, DR readiness and Go-live	T3	T4=T3

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

C) Services Implementation (One time) Timelines:

S.No.	Activity/Milestone	Start date	End Date
1	Milestone 1: SRS, HLD, LLD Signoff of Respective services	T0	T1= T0+1.5 Month
2	Milestone 2: Installation & configuration of software/solution/tools	T0	T2= T0+1.5 Month
3	Milestone 3: UAT & UAT Signoff in bank’s environment	T2	T3= T2+1 Month
4	Milestone 4: Go-live preparedness, and Go-live	T3	T4=T3+0.5 Month

T0- Date of acceptance of PO

Architecture Assessment on a half yearly basis- Within 15 days of bank notifying the bidder to initiate the assessment.

*The timelines provided are indicative, but the *overall implementation period* is non-negotiable. Individual milestones will be discussed and agreed upon with the bank, and the approved dates will be used for tracking progress and calculating SLAs and LDs.

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 Bid evaluation
- ▶ Stage 2 - Evaluation methodology for eligible bidders
 - Technical Bid Evaluation
 - Commercial Bid Evaluation
 - Weighted evaluation (H1)

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.

10.2 Eligibility Evaluation Criteria

Eligibility criteria to be met mandatorily by the bidders:

#	Eligibility Criteria/Clause	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, GST Registration Certificates issued by competent authority in India
4	The bidder should have a minimum turnover of INR 250 crore per annum in India for each of the past 3 financial years (i.e. 2021-22, 2022-23 & 2023-24) along with positive net worth. Note – In case of MSMEs only, the turnover may be relaxed subject to meeting the quality and technical specifications.	CA Certificate mentioning the turnover and net worth for each financial year. and Audited Financial statements (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 OEM in India. MAF should be submitted from the following solution OEMs: i. Centralized Key Management Solution ii. Certificate lifecycle management iii. Information / Digital Rights Management (DRM) iv. Mobile SDK v. IDAM vi. MFA vii. PIM	MAF from the respective OEMs of the solution & services

#	Eligibility Criteria/Clause	Documents
	viii. DAM ix. S-BOM & CBOM x. ITGRC	
6	Bidder must have at least enrolled manpower (on bidder's payroll) of 100 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) any 3 of the below solutions in any one PSU/PSE/ Government Organizations / BFSI in India: <ol style="list-style-type: none"> Centralized Key Management Solution /Certificate Lifecycle management Information / Digital Rights Management (DRM) Mobile SDK IDAM MFA/2FA PIM DAM S-BOM & CBOM IT GRC <p>Note: -</p> <ol style="list-style-type: none"> Experience of DAM and IDAM is mandatory Experience can be shown in single /multiple Clients/work orders meeting the above criteria The above experience/project should not be later than last 5 years from the date of bid opening 	Copy of Purchase Order/Work Order/ Contract AND Client Credential letter highlighting the product and stage of the project/Email Confirmation from the client highlighting the product and stage of the project/Client Signed Installation Report/Client Sign-off.
8	Bidder must have back-to-back support relation with 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

#	Eligibility Criteria/Clause	Documents
		<p>respective solutions & services OEMs proposed through this RFP within 1 month of issuance of the Purchase order.</p> <p>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.</p>
9	<p>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.</p> <p>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</p>	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 should not have been blacklisted at the time of submission of the bid by any regulator / statutory body/ any government department/ PSU/ BFSI in India.	Self-Certification from the bidder as per Annexure 10
12	The bidder should not be involved in any litigation which threatens the solvency of company.	Self-Certification from the bidder as per Annexure 9
13	Labor Law Compliance	Self-Certification from the bidder
14	Integrity Pact	Document on 100 Rs Stamp paper, duly signed and stamped by the authorized signatory.
15	Non-Disclosure Agreement	Document on 100 Rs Stamp paper, duly signed and stamped by the authorized signatory.

#	Eligibility Criteria/Clause	Documents
16	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 or new contract	Self-declaration signed by Authorized Signatory of the bidder.
OEM Evaluation Criteria		
17	<p>The proposed OEM solution should have been implemented in at least two Scheduled Commercial Bank (Including banking Regulator)/PSU/ PSE/Government Organizations / BFSI in India.</p> <p>Credential is to be submitted for the following solutions:</p> <ol style="list-style-type: none"> Centralised Key Management Solution Information / Digital Rights Management (DRM) Mobile SDK IDAM MFA DAM S-BOM & CBOM IT GRC <p>Note: - Experience of solution can be shown in single /multiple Clients/work orders meeting the above criteria Note: The above experience/project should not be later than last 5 years from the date of bid opening</p>	<p>Copy of Purchase Order/Work Order/ Contract AND Client Credential letter/Email Confirmation from client highlighting the product & stage of the project OR Client Signed Installation Report/Client Sign-off OR Self-Declaration from OEM confirming the product & stage of the project</p>
18	Compliance with the FRS, TRS, SoW, SBOM & CBOM	<p>Self-declaration from the respective OEM for each of the products & services as mentioned below. FRS and TRS compliance sheet (Excel) are to be submitted along with the self-declaration.</p> <p>Solution List:</p> <ol style="list-style-type: none"> Centralized Key Management Solution Information / Digital Rights Management (DRM) Mobile SDK

#	Eligibility Criteria/Clause	Documents
		d. IDAM e. MFA f. PIM g. DAM h. S-BOM & CBOM i. IT GRC

In the event that a bidder has submitted proposals for NextGEN SOC and IT Security RFPs, the commercial bid that is opened first (NextGEN SOC or IT Security RFPs) and awarded/identified as the selected bidder, will render them automatically disqualified from the other RFPs. Consequently, the commercial bid of the bidder for the other RFP will not be opened.

Note:

1. Attested photocopies of all relevant documents / certificates should be attached as proof in support of the claims made. The bidder should provide relevant additional information wherever required in the eligibility criteria. PSB reserves the right to verify /evaluate the claims made by the Bidder independently. Any decision of PSB in this regard shall be final, conclusive, and binding upon the Bidder.
2. In case of business transfer where bidder has acquired a Business from an entity (“Seller”), work experience credentials of the Seller in relation to the acquired business may be considered.
3. In the case of corporate restructuring the earlier entity’s incorporation certificate, financial statements, Credentials, etc. may be considered.
4. Either the bidder on behalf of the Principal/OEM or Principal/OEM itself can bid but both cannot bid simultaneously for the said RFP.
5. The bidder/OEM comply with CVC guideline 3 (a,b) circular no. 03/01/12, GFR Rule 16(a) of 2005 and OM of DOE dated 25/07/2016
In a tender, either the Indian agent on behalf of the Principal/OEM or Principal/OEM itself can bid but both cannot bid simultaneously for the same item/product, in the same tender.
6. If an agent submits a bid on behalf of the principal/OEM, the same agent shall not submit a bid on behalf of another principal/OEM in the same tender for the same item/product.
7. Documentary evidence must be furnished against each of the above criteria along with an index. All documents must be signed by the authorized signatory of the Bidder. Relevant portions in the documents submitted in pursuance of eligibility criteria should be highlighted.

10.3 Technical Evaluation Criteria

The technical bid submitted by the Bidder will be evaluated only if they fulfil the eligibility criteria as defined in section 10.2 Eligibility evaluation criteria. The technical bid evaluation will be done with a total score of 100 marks.

Bidders scoring at least the minimum score of 65 marks or more will be declared technically qualified.

The bidders scoring less than 65 marks (cut-off score) out of 100 marks in the technical evaluation criteria defined in the below table shall not be considered for further selection process and their offers will be dropped at this stage.

Detailed Evaluation Criteria:

*Documentary evidence as mentioned in the eligibility criteria's

S.No.	Technical Evaluation Clause	Scoring
Financial Strength		
1	a. Point 1 = 250 Cr. < Minimum turnover of bidder in each of the 3 financial years < 500 Cr. b. Point 2 = 500 Cr. < Minimum turnover of bidder in each of the 3 financial years < 750 Cr. c. Point 3 = Minimum turnover of bidder in each of the 3 financial years > 750 Cr. Financial years (i.e. 2021-22, 2022-23 & 2023-24)	a. Point 1 = 4 b. Point 2 = 5 c. Point 3 = 6 Max Marks – 6
Bidder's Experience		
2	Bidder should have supplied, installed and maintained (or under maintenance) from the following solutions: i. Information / Digital Rights Management (DRM) ii. Mobile SDK iii. IDAM iv. MFA/2FA v. PIM vi. DAM vii. Centralized Key Management Solution/Certificate lifecycle management viii. S-BOM & CBOM	a. Point 1: 6 Marks b. Point 2: 9 Marks Max Marks – 9

S.No.	Technical Evaluation Clause	Scoring
	<p>Point 1: = 3 of the above-mentioned solution in any PSU/ PSE/ Government Organizations / BFSI in India</p> <p>Point 2: ≥ 4 above mentioned solution in any PSU/ PSE/ Government Organizations / BFSI in India</p> <p>Note: - Experience of solution can be shown in single /multiple Clients/work orders meeting the above criteria</p> <p>Note: The above experience/project should not be later than last 5 years from the date of bid opening</p>	
OEM Evaluation Criteria		
3	<p>The proposed OEM solution should have been implemented in at least 2 Clients in India</p> <p>Credential is to be submitted for each of the following solutions:</p> <p>i. Database Access management (DAM)</p> <p>Matrix:</p> <p>a. Point 1: Client 1 - BFSI and Client 2- BFSI</p> <p>b. Point 2: Client 1: PSU/PSE/Govt. Organization in and Client 2- PSU/PSE/Govt. Organization</p> <p>c. Point 3: Client 1 – Scheduled Commercial Bank (Including banking Regulator) and Client 2- PSU/PSE/Govt. Organization/BFSI</p> <p>d. Point 4: Client 1 - Scheduled Commercial Bank (Including banking Regulator) and Client 2- Scheduled Commercial Bank (Including banking Regulator)</p> <p>Note: - Experience of solution can be shown in single /multiple Clients/work orders meeting the above criteria</p> <p>Note: The above experience/project should not be later than last 5 years from the date of bid opening</p>	<p>Category</p> <p>a. Point 1 = 6</p> <p>b. Point 2 = 7</p> <p>c. Point 3 = 8</p> <p>d. Point 4 = 9</p> <p>Max Marks – 9</p>
4	The proposed OEM solution should have been implemented in at least 2 Clients in India	Category

S.No.	Technical Evaluation Clause	Scoring
	<p>Credential is to be submitted for each of the following solutions:</p> <ol style="list-style-type: none"> Centralized Key Management Solution Certification Lifecycle management Information / Digital Rights Management (DRM) Mobile SDK IDAM MFA S-BOM & C-BOM <p>Matrix:</p> <ol style="list-style-type: none"> Point 1: Client 1 - BFSI and Client 2- BFSI Point 2: Client 1: PSU/PSE/Govt. Organization in and Client 2- PSU/PSE/Govt. Organization Point 3: Client 1 – Scheduled Commercial Bank (Including banking Regulator) and Client 2- PSU/PSE/Govt. Organization/BFSI Point 4: Client 1 - Scheduled Commercial Bank (Including banking Regulator) and Client 2- Scheduled Commercial Bank (Including banking Regulator) <p>Note: - Experience of solution can be shown in single /multiple Clients/work orders meeting the above criteria</p> <p>Note: The above experience/project should not be later than last 5 years from the date of bid opening</p>	<ol style="list-style-type: none"> Point 1 = 5 Point 2 = 6 Point 3 = 7 Point 4 = 8 <p>Max Marks – 56</p> <p>Scoring will be conducted for each solution individually and then consolidated to determine the highest overall score.</p>
5	<p>A presentation to be made by the bidder covering the following aspects (but not limited to):</p> <ol style="list-style-type: none"> Capability demonstration by the bidder Understanding of Scope of work & terms of the RFP Proposed Approach and Methodology for implementation Approach & methodology for providing Managed Security Services (MSS) to run IT Security Solution services Solution Description, Functionality, Architecture & Deployment model, Resilience of proposed architecture 	Max Marks – 20

S.No.	Technical Evaluation Clause	Scoring
	<p>f. Resource Deployment plan, Implementation Plan</p> <p>g. Bidder to demonstrate a relevant AI/ML capability use case, models etc.</p> <p>All eligible bidders will be required to make presentations. The bank will schedule presentations, and the time and location will be communicated to the bidders. Failure of a bidder to complete a scheduled presentation to the bank may result in rejection of the proposal</p>	

*Documentary evidence as mentioned in the eligibility criteria's

1. When deemed necessary the Tender Evaluation Committee may seek clarification on relevant aspects from the Bidder. However, that would not entitle the Bidder to change or cause any change.
2. Scores for the above individual parameters shall be added to determine the technical scores of the Bidders. The Bidder with the highest technical score shall be ranked as T1.
3. 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.

10.4 Commercial Evaluation Criteria

The commercial bid of only technically qualified bidders shall be opened. These technically qualified bidders as per technical 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 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 Commercial Bid (CB) with the lowest value will be awarded a financial score (Sf) of 100 points. The financial scores for all other bids will be calculated using the following formula:

$$Sf = 100 \times CB / F$$

(F = amount of Commercial Bid (Last value quoted/entered by the bidder)).

10.5 Final Evaluation – Weighted Techno-Commercial Evaluation

The Proposals will be finally ranked according to their combined Technical Score(s) and Financial Score as follows:

$$S = ST \times Tw + SF \times Fw$$

Where S is the combined score, and Tw and Fw are weights assigned to Technical Proposal and Financial Proposal that shall be 0.70 and 0.30 respectively.

ST and SF will be calculated for individual bidders, as per description mentioned in Evaluation Criteria Section respectively.

Bidder with the highest Final score shall be considered for award of the Contract.

For example:

Three bidders, namely A, B and C, participated in the bid process and their technical scores are as below:

$$A=70, B=85, C=90$$

After converting them into percentile, we get

$$ST \text{ for A} = (70/90) \times 100 = 77.77$$

$$ST \text{ for B} = (85/90) \times 100 = 94.44$$

$$ST \text{ for C} = (90/90) \times 100 = 100$$

The Final prices of the bidders are as under: A= Rs. 8500, B= Rs. 9000, C= Rs. 12000

The final cost quoted by the bidders converted into percentile score shall be as under:

$$SF \text{ for A} = (8500/8500) \times 100 = 100$$

$$SF \text{ for B} = (8500/9000) \times 100 = 94.44$$

$$SF \text{ for C} = (8500/12000) \times 100 = 70.83$$

As the weightage for technical parameter and cost are $T_w = 70\%$ and $F_w = 30\%$ respectively, the final scores shall be calculated as below:

$$S \text{ for A} = (77.77 \times 0.7) + (100 \times 0.3) = 84.439$$

$$S \text{ for B} = (94.44 \times 0.7) + (94.44 \times 0.3) = 94.44$$

$$S \text{ for C} = (100 \times 0.7) + (70.83 \times 0.3) = 91.25$$

Hence, the offer of 'B' (being highest score) will be considered and the contract shall be awarded B' at Rs. 9000 being the final price quoted by B.

Note:

1. The bank will at its own discretion decide to either –
 - Open commercial bids in front of the bidders after the technical evaluation is complete, and calculate the TCO, Or
 - The highest technical bidder shall not automatically qualify for becoming selected bidder and for the award of contract by the bank.
2. The Successful Applicant shall be the first ranked Applicant (having the highest combined score). The final decision on the successful bidder will be taken by the bank. The implementation of the project will commence upon acceptance of purchase order and signing of Contract by the selected bidder.
3. If for some reason, the successful bidder fails to execute an agreement within a specified timeline, the bank reserves the right to award the contract to the next most eligible bidder based on the final evaluation scope of technical evaluation scores and commercial prices quoted.
4. In case of a tie of Total Score between two or more bidders, the Bid with higher technical score would be chosen as the successful Bidder.
5. The bank will calculate the scores up to 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.

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

S. No	Items	Milestone	Percentage
1.	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: <ul style="list-style-type: none"> • 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	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: <ul style="list-style-type: none"> • Delivery proof • OOTB Installation Proof • Invoice of the Product 	50%

S. No	Items	Milestone	Percentage
		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.

11.2 OEM Services Cost

S. No	Items	Milestone	Percentage
	OEM Services Cost	Payable in arrears post providing the service	Quarterly in arrears
4	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
5	Hardware Cost (other than Appliances)	Delivery of hardware and submission of invoice with Proof of Delivery and other documents of the hardware 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).	70%
		On successful installation of at least 50% of the OOTB product/solutions* on the hardware (as detailed in Virtual to Physical mapping -Appendix 3: BoQ) sought by Bank mentioned in the table (Section 7)	20%
		<p>*50% of the OOTB product here refers to the following:</p> <ul style="list-style-type: none"> a. Total Count of product/solutions should be at least 50% of the sought product/solutions as mentioned in the table (Section 7) and b. Total Cost (as per the Appendix 2: Commercial Bill of Material) of the product/solutions should be at least 50% of the total product cost sought as mentioned in the table (Section 7) 	
		On successful installation of remaining 50% of the OOTB	10%

S. No.	Items	Milestone	Percentage
		products/solutions on the hardware	
6	Hardware Cost (For Appliance)	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. The Bidder is required to submit the required to submit the following: <ul style="list-style-type: none"> • 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%

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
7	ATS/ Annual Subscription & AMC Cost	ATS/ Annual Subscription Cost	Yearly in advance (Post submission of 110% of the yearly ATS Amount of the respective product) or quarterly in arrears
8		AMC	Yearly in advance (Post submission of 110% of the yearly AMC Amount of the respective product) or quarterly in arrears

11.5 Facility Management (FM) Cost:

(FM manpower Support for maintaining and managing the application, IT Infrastructure and other terms of the RFP)

S. No	Items	Milestone	Percentage
9	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
10	Other Cost	Payable in arrears	After completion of respective activity

Note:

- a. Annual Maintenance Contract (AMC)/ Annual Technical Support (ATS) includes all hardware, software, applications, services deployed in the IT Security
- 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 is bound and to comply the Service Levels as described below-

1. The successful bidder shall have to enter into the "Service Levels Agreement" having all terms and conditions of this RFP to maintain uptime and provide the service support and onsite support during the entire contract period.
2. Both the bidder and OEM will be totally responsible for the maintenance, configuration and fault-free operations of supplied infrastructure, i.e. hardware, software and its maintenance during the AMC/ATS period.
3. Any technical glitch/ issue in installed infrastructure of the solution (i.e. hardware and software, OS/DB etc.) should be attended on priority and should be covered under warranty/AMC.
4. The bidder has to maintain a guaranteed minimum uptime for all systems/ solutions supplied under this RFP to avoid any business disruption due to breakdown of system or degraded performance impacting on business or unavailability of data. The calculation of uptime will be monthly.
5. The issue/ break down message may be communicated to/by the Bank team by way over phone / email/ call logging.
6. For penalty calculation, the total time elapsed between the intimation of break down message from Bank side to the bidder and receipt of rectification message from the bidder to Bank side will be considered.
7. The penalty will be deducted in quarterly FMS/AMC/ATS payment. In case the Bank is unable to adjust penalty in FMS/AMC/ATS payment, the Bank at its discretion may invoke the Performance Bank Guarantee (PBG) to deduct the penalty amount.
8. If the support services are not provided on 24*7 basis and/or satisfactory services are not provided as sought in the RFP, the Bank with its discretion may reject the proposal/ terminate the contract, without assigning any reason.
9. The bidder is required to mandatorily conduct quarterly preventive and breakdown maintenance activities to ensure (without any impact on day-to-day operations) maintaining uptime on a monthly basis covering 24*7*365 days.
10. The business hours are 6 AM to 10 PM on any calendar day the Bank 's branch is operational. The Bidder, however, recognizes the fact that the branches will require them to work beyond the business hours and holidays on need basis
11. Apart from maintaining uptime, for any breakdown / malfunctioning of hardware and it's any of the components or accessories or any system software issue etc., the resolution time is mentioned below: -

$$\text{Uptime \%} = ((\text{Number of hours in month} - \text{Number of hours impacted in month}) * 100) / (\text{Total Number of hours in month})$$
12. For calculation of uptime (penalty), planned/ scheduled down time will be exempted. Bank will pay the bidder after deducting the calculated penalty from the payable amount.
13. If any critical component of the entire configuration setup is out of service, then the bidder & OEM shall either immediately replace the defective unit (with new one) or replace it at its own cost or provide a standby, on an immediate basis, not more than 4 hours, The bidder should maintain proper inventory of standby components for early resolution of issues.
14. If the bidder, having been notified, fails to remedy the defect(s) within the 4 hours' time duration from the incident, the Bank may proceed to take such remedial action as may be necessary, at the Supplier's risk and expense and without prejudice to any other rights, which the Bank may have against the supplier under the Contract.

15. The bidder should comply with the security and audit standards of the Bank and various regulatory guidelines. For this, the bidder should apply new patches related to OS/ firmware & BIOS updates etc, without any additional cost to the bank, during the contract period.
16. For all issues related to the solution supplied by the bidder, RCA (Root Cause Analysis) from the respective OEM to be provided by the bidder within 3 working days. The delay in submission of RCA will lead to penalty Rs. 20000/day

Level Classifications

Level	Function/Technologies	Typical Response & Resolution Time
Critical /High	<p>i Such a class of errors will include problems, which prevent users from making operational use of solutions and impact the other solutions functioning.</p> <p>ii All the proposed solutions, IT Infrastructure and proposed services</p> <p>iii Security Incidents</p> <p>iv No work-around or manual process available</p> <p>v Financial/reputational impact on Bank</p> <p>vi Infrastructure related to providing solutions to the Bank users comprising of but not limited to the following:</p> <ul style="list-style-type: none"> Proposed Solution Tools / IT Infrastructure application servers/infra Proposed Solution Tools / IT Infrastructure web servers/infra Proposed Solution Database Servers / Appliance Proposed Solution servers/appliances Network components, if any proposed by the bidder 	<p>During business hours – Response Time: Within 30 minutes Resolution Time: Within 120 minutes</p> <p>Non - business hours – Response Time: Within 30 minutes Resolution Time: Within 4 hours or earlier as per business hours if business hours begin</p> <p>For the Business, Network & Security Infrastructure & Systems procured by the Bank from Third party Vendor or for the services where the Bank has direct contract with the 3rd Party Vendor,</p> <p>Bidder shall ensure that the calls are logged with the respective Vendor within 30 minutes of occurrence of such incidents post identification of the issue.</p>
Key / Medium	<p>i Any incident which is not classified as “Critical” for which an acceptable workaround has been provided by the Bidder or;</p> <p>ii Any problem due to which the infrastructure of the proposed solution is not available to the Bank users or does not perform according to the defined performance and query processing parameters required as per the RFP or;</p> <p>iii Users face severe functional restrictions in the application irrespective of the cause.</p> <p>iv Key business infrastructure, systems and support services comprising of but not limited to the following:</p> <ul style="list-style-type: none"> Proposed solution non-production environment (Test & Development and Training Infrastructure) 	<p>During business hours – Response Time: Within 30 minutes Resolution Time: Within 240 minutes</p> <p>Non-business hours – Response Time: Within 30 minutes Resolution Time: Within 6 hours or earlier as per business hours if business hours begin</p> <p>For the Business, Network & Security Infrastructure & Systems procured by the Bank from Third party Vendor or for the services where the Bank has direct contract with the 3rd Party Vendor, Bidder</p>

Level	Function/Technologies	Typical Response & Resolution Time
		shall ensure that the calls are logged with the respective Vendor within 15 minutes of occurrence of such incidents post identification of the issue.
Significant/ Low	<ul style="list-style-type: none"> i Any incident which is not classified as “key” or “critical” for which an acceptable workaround has been provided by the Bidder. ii Moderate functional restrictions in the application irrespective of the cause. It has a convenient and readily available workaround. iii No impact on processing of normal business activities iv Equipment/system/Applications issues and has no impact on the normal operations/day-to-day working. v All other residuary proposed solution Infrastructure not defined in “Critical” and “key” 	<p>During business hours – Response Time: Within 30 minutes Resolution Time: Within 6 hours.</p> <p>Customizations-Time period decided by mutual agreement. Scheduled monitoring activities decided by mutual agreement. Response and resolution time for Bank infrastructure should be 1 working day.</p> <p>Response and resolution for other criteria- During business hour – within 4 hours. Non- Business Hours- The issue has to be resolved on the next business day adhering within 4 hours.</p>

Service Levels

Service Levels will include Availability measurements and Performance measurements parameters.

The bidder shall provide the Availability Report on a monthly and quarterly basis and a review shall be conducted based on this report. A monthly report shall be provided to the BANK at the end of every month containing the summary of all incidents reported and associated with Bidder performance measures for that period. Performance measurements would be assessed through audits or reports, as appropriately to be provided by Bidder e.g. utilization reports, response time measurements reports, etc. 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.

Monthly Maintenance Cost	=	$\frac{\text{Total FM(O\&M) Manpower Cost} + \text{Total AMC of Infrastructure/appliance} + \text{Total ATS or Subscription cost of proposed software's/tools}}{\text{Support Period in years} * 12}$
--------------------------	---	---

Quarterly Maintenance Cost	=	$\frac{\text{Total FM(O\&M) Manpower Cost} + \text{Total AMC of Infrastructure/appliance} + \text{Total ATS or Subscription cost of proposed software's/tools}}{\text{Support Period in years} * 4}$
----------------------------	---	--

Availability Measurements

Level	Type of Infrastructure	Measurement	Minimum Service Level	Penalty
Cyber Security Solutions and IT Infrastructure (HCI/Virtualization, OS, DB, IT Components Etc.) for Cyber security solutions	Proposed Infrastructure & Systems	Availability of each solution, Infrastructure Elements & Systems, any individual component	99.90%	For every 0.05% or part thereof drop in service levels penalty will be 1% of the Monthly Maintenance Cost The Calculation of penalty will happen based monthly performance data as received

- Availability Service Level will be measured monthly.
- The Bidder's performance to Availability Service Levels will be assessed against Minimum Service Level requirements monthly for each criterion mentioned in the Availability measurement table.
- An Availability Service Level Default will occur when: The Bidder fails to meet Minimum Service Levels, as measured monthly, for a particular Service Level.

Services SLAs:

Service Area	Service Level	Penalty
Each Proposed Services Uptimes	99.90%	For every 0.05% or part thereof drop in service levels penalty will be 1% of the Monthly Maintenance Cost Service level drop below 90%, penalty shall amount to 100% of the Monthly Maintenance Cost

The mechanism for monitoring the SLA would need to be proposed by the bidder and agreed by the BANK.

Performance Measurements

Performance Measurements will be made on a monthly basis or as required by BANK.

Type of Infrastructure	Measurement	Minimum Service Level	Measurement Tools	Penalty
Hardware Utilization	<p>The daily peak utilization of CPU RAM, NIC and Hard disk etc. of the specific hardware (including each VM) exceeds 75% at any given point of time. Each incident should not exceed 5 minutes, or part thereof will be a new incident.</p> <p>In case VMs are created on the physical Hardware, Utilization SLA would also be monitored at each VM/container and utilization of each VM/Container should also not cross 75% at any given point of time. Each incident should not exceed 5 minutes, or part thereof will be a new incident.</p>	100%	Each Incident Reporting	<p>If less than 3 times in a month: for every incident in service level, Penalty of 1% of the monthly maintenance cost.</p> <p>If there are more than 3 times in a month: Bidder will be responsible for replacing/augmenting the hardware at no additional cost to the BANK within 3 months of exceeding the thresholds.</p> <p>In-case bidder fails to replace the hardware, LD (over and above the penalty for incident breaching during the replacement or augmentation period for each incident) of 1% of affected product cost will be levied for every week of delay or part thereof. Till the replacement/augmentation is done the bidder has to provide the alternative infrastructure to ensure compliance to the service during the replacement/augmentation period.</p>
Storage Utilization	If the daily peak utilization level exceeds 80% at any given point of time and such incidents occur more than 3 times in a month. Each incident should not exceed 5	100%	Each Incident Reporting	<p>If less than 3 times in a month: for every incident in service level, Penalty of 1% of the monthly maintenance cost.</p> <p>If more than 3 times a month: Bidder will be responsible for replacing/augmenting the</p>

Type of Infrastructure	Measurement	Minimum Service Level	Measurement Tools	Penalty
	minutes, or every part thereof will be a new incident.			<p>hardware at no additional cost to the BANK within 3 months of exceeding the thresholds.</p> <p>In case, the bidder fails to replace the hardware, LD (over and above the penalty for incident breaching during the replacement or augmentation period for each incident) of 1% of affected product cost will be levied for every week of delay or part thereof. Till the replacement/augmentation is done bidder has to provide the alternative infrastructure to ensure the compliance to the service during the replacement /augmentation period.</p>
Disaster Recovery Instance Availability	<p>Business operations to resume from Disaster Recovery Site within defined RTO and RPO from data Centre failing/down. Specific RTO and RPO are defined below</p> <ul style="list-style-type: none"> Recovery Point Objective (RPO) is 30 minutes Recovery Time Objective (RTO) is 60 minutes 	100% (Instance Wise)	BANK will measure through Periodic audits and reports	INR 10,000 for every 10 Minutes of delay above defined RPO and RTO

Incident Management

Services	Description	Calculation	Periodicity	MSL	Penalty
Incident logging	Bidder shall ensure that all incidents reported by the users / testing team shall be duly logged and assigned to teams with a unique ID for reference purposes. Users shall be informed about the reference ID maximum within 30 minutes from recording the complaint	Manually through various communication channels	Monthly	100%	Penalty of INR 10,000 will be levied for every 30 minutes delay or part thereof
Incident resolution within targets	This Service Level measures the number of all category calls/ incidents per month that get resolved within the response time & resolution time defined divided by the total number of calls that get logged	Call Tickets per month responded and resolved within the timelines divided by the total number of call tickets per month	Monthly	100%	<p>Business hours- For every 0.5% drop in service level or part thereof, Penalty shall be 0.5% of the monthly maintenance Cost</p> <p>Non-Business Hours For every 1% drop in service level or part thereof, Penalty shall be 0.5% of the monthly maintenance Cost</p>

Management, Reporting and Governance

Service Details	SLA Measurement	SLA	Penalty	Remarks
Key Resources	Any change during the contract period	100%	More than 1 change would lead to a penalty of INR 2,00,000 for each default for each key resource	

Service Details	SLA Measurement	SLA	Penalty	Remarks
Manpower availability	Bidder to provide experienced manpower at Bank premises as per requirement mentioned RFP.		<ul style="list-style-type: none"> <80% of required strength -- Rs. 25,000/- per resource per week or part thereof <60% of required strength -- Rs. 50,000/- per resource per week or part thereof <35% of required strength -- Rs. 1 Lakh per resource per week or part thereof from the day of breach of SLA until the required strength is achieved. 	<p>Service Level Agreements (SLAs) will be calculated on a monthly basis, based on the availability of the resources during that month.</p> <p>Absence of any resource must be complemented with an equally skilled resource.</p>
Report Generation	Adherence to delivery of SLA report	100%	<p>The SLA reports are to be shared with the BANK by the 7th of every month.</p> <p>For each default the penalty of INR 20,000 per week or part thereof may be charged to the bidder</p>	<p>The indicative list of required reports is mentioned in RFP. However, BANK may add or remove reports as at its discretion.</p>
Security Device Management and Administration	Bidder is expected to provide this service 24/7 on a 24-hour basis. Management and administration of all in-scope security devices and/or solutions	100%	<p><u>Penalty:</u></p> <ul style="list-style-type: none"> For wrong rule modification (as approved by BANK) in any of the security solutions will incur a penalty of INR 20,000 for each default. For a wrong rule modification (as approved by BANK) in any of the security solutions by which BANK incur any service disturbance will incur a penalty of INR 30,000 for each default. 	

Security Vulnerability Management:

Service Area	Service Level	Penalty
Version Upgrade Major/ Minor for all Software/ Middleware/ OS (All version) and Patching of all Hardware/ Software/ Middleware/ OS (All version)	<p>The Operations Team has to have version upgrades /patching of all underlying software / hardware/ Middleware as per respective OEM recommendations & publish the Monthly version/Patch upgrade calendar for the same.</p> <p>Failure to comply with the Version upgrade/patches etc. calendar will attract penalties.</p> <p>SLA related to this will start after 1 month's post signoff</p>	<p>For breaches of Version upgrade/patching –</p> <ul style="list-style-type: none"> 95-100 % -- No penalty Below 95 %-- INR 500 per day will be deducted per percentage of non-compliance till the approved upgrades/updates/patches are applied in the system

Management & health checkup:

Service Area	Service Level	Penalty
OEM Involvement	Review to be conducted by OEM	Penalty of Rs. 2,00,000 per day for each such a solution for each default would be imposed.
Open OEM Support tickets/cases	Closure of OEM Support tickets within 2 weeks	<p>Unable to close the OEM support tickets within 2 weeks without any workaround</p> <p>1% of overall monthly maintenance cost per week for non-compliance after the timelines</p>
Compliance of RBI/ CERT-IN Advisories/ other regulatory advisory	Compliance by end date, as notified in the advisory	Compliance by end date - No Penalty
	Penalty by delay by each day.	By Delay of each day, 0.5% of Monthly Contract Value, per day

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

Item	Issue Categorization	Resolution Period	Penalty Amount
Audit Gaps Resolution	Critical	Within 1 Month	INR 16,000 per issue per day post the resolution period till the issue/gap closure date
	High	Within 1 Month	INR 8,000 per issue per day post the resolution period till the issue/gap closure date
	Medium	Within 2 Months	INR 5,000 per issue per day post the resolution period till the issue/gap closure date
	Low	Within 3 Months	INR 3,000 per issue per day post the resolution period till the issue/gap closure date

****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 13.12 for LD on Supply & Delivery

Installation & Implementation

If the bidder fails to Implement solution and/or services within the time period(s) specified in the Delivery Schedule or implementation, 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 percent per week or part thereof of respective new/ Existing 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 (new/existing) here defined as the sum of Product license cost and product implementation 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 or permit anyone to perform any of the work, service or other performance required under the contract other than the L1 Resources services (O&M Phase).
2. 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 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:

- a. Claiming Liquidated Damages
- b. Termination of the purchase agreement fully or partly and claim liquidated damages.
- c. Execution of Bid Declaration Form / Invoking EMD or Performance Bank Guarantee

13.3 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.

13.4 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.

13.5 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.

13.6 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.

13.7 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 25 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.

13.8 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.

13.9 Indemnity

The Service Provider 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 claim for infringement of intellectual property rights.

The Service Provider 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 Service Provider agrees to indemnify and keep indemnified Bank at all times against all claims, demands, actions, costs, expenses (including legal expenses), loss of reputation and suits which may arise or be brought against the Bank, by third parties on account of negligence or failure to fulfil obligations by the selected Service Provider or its employees/personnel.

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

13.10 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:-

1. Natural phenomenon, including but not limited to floods, droughts, earthquakes, epidemics and pandemics
2. Acts of any government, including but not limited to war, declared or undeclared priorities, quarantines and embargos
3. Terrorist attack, public unrest in work area
4. 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.
5. 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.
6. As soon as the cause of force majeure has been removed, the Bidder shall notify the Bank and resume the affected activity without delay.
7. Notwithstanding the above, the decision of the bank shall be final and binding on the Bidder in the event of force majeure.

13.11 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.

13.12 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.

13.13 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.

13.14 Liquidated Damages

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

13.15 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, 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.

13.16 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 forgoing, 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.

13.17 Order Cancellation

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) and recover expenditure incurred by the Bank in addition to recovery of liquidated damages in terms of the contract, in the event of one or more of the following conditions:
 - a) Delay in delivery of services in the specified period.

- b) Serious discrepancies are noted in the inspection.
 - c) Breaches in the terms and conditions of the Order.
2. The Bank reserves the right to cancel the contract placed on the selected bidder and recover the expenditure incurred by the Bank on the following circumstances:
 - 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 10% of the total contract price.
 - h) If found blacklisted by any Govt. Department / PSU / other Banks / CERT-In, during contracted period.
 - i) 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.
3. In case of Implementation delay by the bidder beyond the specific period (*i.e., Implementation Period + Cure Period granted by the bank*), the Bank shall have the right to recover from the Bidder any amounts already paid by the Bank in respect of the product/solution concerned (including related hardware) and/or services, after duly adjusting for any penalties already levied and recovered by the Bank for that specific product or service. However, if the Bidder can provide satisfactory evidence to the Bank that the delay, deficiency, or default was not attributable to the Bidder, such portion shall be excluded from the scope of recovery.
4. Bank shall serve the notice of termination to the bidder at least 30 days prior of its intention to terminate services without assigning any reasons.
5. In case the selected bidder fails to conduct an event as per stipulated schedule, the Bank reserves the right to get it conducted by alternate sources at the risk, cost and responsibility of the selected bidder by giving 7 days' prior notice to the bidder.
6. After the award of the contract, if the selected bidder does not perform satisfactorily or delays execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving one-month notice for the same. In this event, the selected bidder is bound to make good the additional expenditure, which the Bank may have to incur to carry out for the execution of the balance of the order/contract. Such additional expenditure shall be incurred by the bank within reasonable limits & at comparable price prevailing in the market. This clause is also applicable if for any reason, the contract is cancelled.
7. The Bank reserves the right to recover any dues payable by the selected bidder from any outstanding amount to the credit of the selected bidder, including the pending bills and security deposit, if any, under this contract.
8. In addition to the cancellation of purchase order, the Bank reserves its right to take appropriate action on the bidder for non- performance and/or invoke the Bank Guarantee or foreclose the Security Deposit given by the bidder towards non- performance/non-compliance of the terms and conditions of the contract, to appropriate towards damages

13.18 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.

13.19 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 agreements 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.

13.20 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.

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 and shall be considered null and void

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: Bill of Quantity

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)

Checklist			
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 formatio 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 1B , 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 IT Security Solutions and Services

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)

Deputy 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 IT Security Solutions and Services

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 _____, 2025

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,

Deputy 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 _____

We have carefully gone through the contents of the above-referred RFP along with replies to pre-bid queries & amendment, if any, and furnish the following information relating to Pre-Qualification Criteria.

- The bidder/OEM comply with CVC guideline 3(a,b) circular no. 03/01/12, GFR Rule 16(a) of 2005 and OM of DOE dated 25/07/2016
In a tender, either the Indian agent on behalf of the Principal/OEM or Principal/OEM itself can bid but both cannot bid simultaneously for the same item/product, in the same tender.
- If an agent submits bid on behalf of the principal/OEM, the same agent shall not submit a bid on behalf of another principal/OEM in the same tender for the same item/product.

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: Manufacturer's Authorization Form

MANUFACTURER'S AUTHORIZATION FORM

RFP No:

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

To,

Deputy 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 IT Security Solutions and Services vide RFP No: _____

We, who are established and reputable manufacturers / producers of _____ having factories / development facilities at _____ (address of factory / facility) do hereby authorize M/s _____ (Name and address of Authorized Business Partner (ABP)) to submit a Bid and sign the contract with you against the above RFP.

1. We hereby extend our full warranty for the Products and services offered by the above _____ against the above RFP.
2. We also undertake to provide any or all of the following materials, notifications, and information pertaining to the Products supplied by the _____:
 - a. Such Products as the Bank may opt to purchase from the _____, provided that this option shall not relieve the ABP of any warranty obligations under the RFP; and
 - b. In the event of termination of production of such Products:
3. Advance notification to the Bank of the pending termination, in sufficient time to permit the Bank to procure needed requirements; and following such termination, furnishing at no cost to the Bank operations manuals, standards and specifications of the Products, if requested.
4. We duly authorize the said _____ to provide on our behalf in fulfilling all installations, technical support and maintenance obligations required by the contract.
5. We hereby certify that we have read the clauses contained in O.M. No. 6/18/2019-PPD, dated 23.07.2020 order (Public Procurement No. 1), order (Public Procurement No. 2) dated 23.07.2020 and order (Public Procurement No. 3) dated 24.07.2020 regarding restrictions on procurement from a

bidder of a country which shares a land border with India. We further certify that we are not from such a country or if from a country, have been registered with competent authority. We certify that we fulfil all the requirements in this regard and our ABP is eligible to participate in the above RFP.

6. We hereby extend our full guarantee and warranty as per terms and conditions of the Bid and the contract for the equipment, solution, and services offered against this invitation for Bid offer by the above firm. We undertake to provide back-to-back support for spare and skill to the bidder for subsequent transmission of the same to the Bank. We also undertake to provide support services during warranty as well as AMC/ATS period if the above bidder authorized by us fails to perform in terms of the RFP.

Yours faithfully

Authorized Signatory

(Name of manufacturers):

Place:

Name:

Date:

Phone No.:

Fax:

E-mail:

15.8 Annexure 8: Certification on OEM Requirements

RFP No:

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

To,

Deputy 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 for Supply Installation, Implementation, Maintenance & Management of IT Security Solutions and Services 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 Bank 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 Bank 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 IT Security Solutions and Services

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,

Deputy 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 IT Security Solutions and Services

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 Government / Government agency / Banks / Financial Institutions in India during last 3 years.

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. xx:xx dated dd/mm/yyyy

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 2025

(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:

- a) "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.
- b) 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.
- c) 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:
 - i) is or subsequently becomes legally and publicly available without breach of this Agreement by either party,
 - ii) was rightfully in the possession of the Bidder without any obligation of confidentiality prior to receiving it from Punjab & Sind Bank,
 - iii) was rightfully obtained by the Bidder from a source other than Punjab & Sind Bank without any obligation of confidentiality,
 - iv) 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.
 - v) the recipient knew or had in its possession, prior to disclosure, without limitation on its confidentiality.
 - vi) 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

- 5) Non-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.
 - 6) 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.
 - 7) 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.
 - 8) 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

- 9) 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.
- 10) 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).
- 11) 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.
- 12) 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.
- 13) Governing Law: Governing Law: The laws of India shall govern this Agreement
- 14) 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.
- 15) 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
- 16) 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:-
 - a) Natural phenomenon, including but not limited to floods, droughts, earthquakes, epidemics and pandemics
 - b) Acts of any government, including but not limited to war, declared or undeclared priorities, quarantines and embargos
 - c) Terrorist attack, public unrest in work area
 - d) 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.
- e) 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.
 - f) As soon as the cause of force majeure has been removed, the Bidder shall notify the Bank and resume the affected activity without delay.
 - g) Notwithstanding the above, the decision of the bank shall be final and binding on the Bidder in the event of force majeure.
- 17) 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, 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.
 - 18) General: The Bidder shall not reverse - engineer, decompile, disassemble or otherwise interfere with any software disclosed hereunder.
 - 19) 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.
 - 20) 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.
 - 21) 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,

Deputy 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 IT Security Solutions and Services 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. "Not withstanding 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 14.30 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 _____ 2025 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,

Deputy 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 _____ 2025

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. Asha Ram Sihag and 2. Aditya Prakash Mishra 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 on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions

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

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

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

e. The Bidder(s)/ Contractor(s) will, when presenting 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 IPC/ PC 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)

(For & On behalf of Bidder / Contractor)

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 OEM's on their letter head)

To,

Deputy 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 for Supply Installation, Implementation, Maintenance & Management of IT Security Solutions and Services vide RFP No: _____

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

S.No.	Product name as per RFP	Product name as per OEM

1. We confirm that we comply with the FRS & TRS requirement **(with at least 75% of the requirement being met through our standard features available in our product)** stated in the RFP and are attaching the Excel/PDF of compliance
2. We confirm that we comply with the SoW requirement stated in the RFP for our product.
3. Attached is the S-BOM & C-BOM (Public) of our solution in the format Annexure 20: S-BOM & CBOM. We shall share private S-BOM & C-BOM (Version that includes sensitive or confidential information, such as vulnerabilities, that should be accessed only by authorized parties) post the issuance of PO. We confirm that we will facilitate through various channels and formats allowing the automated and secure exchange of SBOM data between different systems or platforms

Yours faithfully

Authorized Signatory

(Name of manufacturers):

Place:

Name:

Date:

Phone No.:

Fax:

E-mail:

15.19 Annexure 19: Stack Confirmation Sheet

Solution:

S.No	Solution Name	Make of the Product	Model of the Product
1	DRM (Digital Rights Management)		
2	Centralized Key Management		
3	Certificate Lifecycle management		
4	S-BOM & C-BOM (Software and Code Bill of Materials)		
5	DAM (Database Activity Monitoring)		
6	Mobile SDK (Software Development Kit)		
7	IDAM (Identity and Access Management)		
8	IT GRC (Governance, Risk & Compliance)		
9	Multi-Factor Authenticator		
	PIM (Privileged Identity Management)		

IT Infrastructure:

S.No	Component Name	Make of the Service Provider
1	Server	
2	Storage	
3	SAN Switch	
4	ToR Switch	
5	Racks	
6	
7	
8	
9	
10	

The details should be in conformity with the **Masked Bill of Material (Appendix 3: Bill of Quantity)** submitted.

Bidders are advised to propose the firm make/model of the products or services. Submission of bids containing alternate options or substitutions in any component is not permitted and bids are liable for rejection.

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

#	Solution Name	Volumetrics
1.	Non-Production Environment	<ul style="list-style-type: none"> The non-production Environment should be 15% of the DC- Primary (whether proposed on-premises or on-cloud) in terms of Compute and Storage

Archived data / logs need to be restored in the respective technology for forensic purpose etc.

The bidder is responsible to provide the correct sizing of compute, network, and storage, IOPS, servers etc. in collaboration with Infrastructure OEM and proposed solution/service OEM whose solution/technologies are proposed for IT Security for successful deployment.

All the necessary cables/SFP's etc. should be factored by the bidder to connect the servers/devices in DC and DR. Bank will provide the leaf switch (Model - Cisco - 93108/93180) ports for connectivity.

Bidder and OEM should also account for scalability and future growth of the Bank to arrive at sizing for the Contract period.

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.

IT Security Solution Details

S. NO	Description	OEM MAKE	OEM MODEL
1	Database Activity Monitoring*	McAfee "Trellix"	MFE Data Centre SEC Suite Dbase
2	Information / Digital Rights Management*	BlackBerry	Blackberry Workspaces
3	SDK for Mobile Access Security*	Checkpoint	Sandblast App Protect
4	Privilege Identity Management Solution (PIM)*	ARCON	U16

***Implemented**

Existing and Envisaged Solutions:

A. Existing Solution Stack:

Perimeter Security	Perimeter Firewall	DDoS	SSL*	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 Decoy	SOAR	AI/ML/UEBA NSPM	ITGRC	Threat Intelligence Platform	Vulnerability lifecycle & Management			

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

15.22 Annexure 22: Client References Format

Format for Submission of Client References

To whosoever it may concern

Particulars	Details
Client Information	
Client Name	
Client address	
Name of the contact person and designation	
Phone number of the contact person	
E-mail address of the contact person	
Project Details	
Name of the Project	
Start Date of the project	
End Date of the project	
Current Status (In Progress / Completed)	
Size of Project	
Value of Work Order (In Lakh) (only single work order)	
Scope of work	
Brief Scope of work relevant to the Bank's (PSB) RFP Requirement	
Cyber Security Solution Scope includes out of the below 1. DRM (Digital Rights Management) 2. Centralized Key Management 3. S-BOM & C-BOM (Software and Code Bill of Materials) 4. DAM (Database Activity Monitoring) 5. Mobile SDK (Software Development Kit) 6. IDAM (Identity and Access Management) 7. IT GRC (Governance, Risk & Compliance) 8. Multi-Factor Authenticator 9. PIM (Privileged Identity Management)	
No. of Branches/offices	
Supporting Document to substantiate the Scope of work	Contract Copy/PO/Credential letter/ Email Confirmation/ Self Declaration (for OEMs)

Name & Signature of authorised signatory

Seal of Company

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	
3	Educational Qualification	
	Degree Obtained	University/ Institution
		Year Obtained
4	Cybersecurity Certification/Qualifications	
5	Professional Experience	
	Designation	Company Name
		Year Obtained
6	Total Years of Cyber Security Experience	
7	Cyber Security Solution and the relevant Project from the below solution 1. DRM (Digital Rights Management) 2. Centralized Key Management 3. Certificate Lifecycle management 4. S-BOM & C-BOM (Software and Code Bill of Materials) 5. DAM (Database Activity Monitoring) 6. Mobile SDK (Software Development Kit) 7. IDAM (Identity and Access Management) 8. IT GRC (Governance, Risk & Compliance) 9. Multi-Factor Authenticator 10. PIM (Privileged Identity Management)	
8	Experience relevant to the Project Wise	

--	--

15.25 Annexure 25: 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 REREFENCE NUMBER: _____

Date:

To,

Deputy 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: