



Central Bank of India

Department of Information Technology

Tender No. GEM/2024/5595196

Request for Proposal (Bid) Document

For

**Supply, Installation and Maintenance of Cybersecurity
Solutions and Associated Hardware at the Bank**

Table of Contents

1. Invitation for Tender Offers.....	8
2. Eligibility Criteria.....	11
3. EMD / Bid Security.....	14
4. Performance Bank Guarantee	14
5. Cost of Bidding.....	15
6. Manufacturer’s Authorization Form	15
7. Scope of Work	16
7.1 Detailed Scope of Work	20
7.1.1 Data Discovery & Classification.....	21
7.1.2 File Upload Security	22
7.1.3 Attack Surface Management (ASM).....	22
7.1.4 Breach and Attack Simulation (BAS) with Red team solution.....	24
7.1.5 Phishing Simulation.....	25
7.1.6 AD Security.....	26
7.1.7 IT Governance, Risk and Compliance (GRC).....	27
7.1.8 Decoy (Honeypot)	28
7.1.9 Mobile Device Management (MDM)	29
7.1.10 Secure Data Backup and Recovery (Ransomware Protection)	31
7.1.11 Network Access Control (NAC).....	31
7.2 Detailed Scope of work for Facility Management Services	33
8. General Responsibility of the Bidder.....	34
9. Project Timelines	36
10. Staggered delivery of the equipment’s.	36
11. Repeat Order (Right to Alter Quantities).....	36
12. Contract Renewal	36
13. SLA compliance.....	37
14. Liquidated damage	44
15. Land Border Sharing Clause	45
16. Monitoring & Audit.....	46
17. Bid Submission	46
18. Integrity Pact	48
19. Commercial Offers	48

20.	Evaluation & Acceptance.....	49
21.	Evaluation Process	49
21.1	Eligibility Criteria Evaluation.....	49
21.2	Technical Evaluation Criteria	50
21.3	Commercial Evaluation Criteria	52
22.	Payment Terms.....	53
22.1	Procedure for Claiming Payments.....	53
22.2	AMC/ATS Payment Terms	54
23.	AMC & ATS and Warranty Costs	54
24.	Order Cancellation	57
25.	Indemnity.....	57
26.	Confidentiality & Non-Disclosure.....	60
27.	Force Majeure	60
28.	Resolution of Disputes	61
29.	Independent Contractor	61
30.	Assignment.....	62
31.	Execution of Contract, SLA & NDA	62
32.	Vendor's Liability	62
33.	Information Ownership.....	63
34.	Inspection, Audit, Review, Monitoring & Visitations	63
35.	Information Security	64
36.	Intellectual Property Rights	65
37.	Termination.....	66
38.	Privacy & Security Safeguards	68
39.	Governing Law and Jurisdiction	68
40.	Compliance with Laws.....	68
41.	Violation of Terms	69
42.	Corrupt & Fraudulent Practices	69
43.	Publicity	69
44.	Entire Agreement; Amendments	69
45.	Survival and Severability	70
46.	Amendments to Bidding Documents	70
47.	Period of Validity	70
48.	Ownership, Grant and Delivery	70

49. Last Date and Time for Submission of Bids.....	71
50. Late Bids.....	71
51. Modifications and/or Withdrawal of Bids	71
52. Signing of Contract.....	71
53. Checklist for Submission.....	72
54. Annexure 1: Bill of Material.....	74
55. Annexure 2: Minimum Technical Specifications	102
56. Annexure 3: Conformity Letter	181
57. Annexure 4: Masked Commercial Bill of Material.....	182
58. Annexure 5: Bidder's Information.....	183
59. Annexure 6: Letter for Conformity of Product as per RFP	185
60. Annexure 7: Undertaking for Acceptance of Terms of RFP	186
61. Annexure 8: Manufacturer's Authorization Form	187
62. Annexure 9: Integrity Pact.....	188
63. Annexure 10: Non-Disclosure Agreement	193
64. Annexure 11: Performance Bank Guarantee	197
65. Annexure 12: Bid Security (Earnest Money Deposit).....	199
66. Annexure 13: Bidder's Particulars.....	201
67. Annexure 14: NPA Undertaking	202
68. Annexure 15: Undertaking letter (Land Border Sharing)	203
69. Annexure 16: Cover Letter.....	205
70. Annexure 17: Pre-bid Query Format	206
71. Annexure 18: Eligibility Criteria Compliance.....	207
72. Annexure 19: Guidelines on banning of business dealing	210
73. Annexure 20: Compliance Certificate with respect to RBI's "Master Direction on Outsourcing of Information Technology Services"	219

Definitions and Acronyms

Following terms are used in the document interchangeably to mean:

Acronym	Definition
AAA	Authentication, Authorization and Accounting framework in Networking
AD	Active Directory
AMC	Annual Maintenance Contract
API	Application Programming Interface
ASM	Attack Surface Management
ATS	Annual Technical Support
Bank/CBoI	Central Bank of India
BAS	Breach and Attack Simulation
"Bidder"	Single point of contact appointed by the Bank for procurement and supply of the equipment based on the Bill of Materials shared by the Bank.
"CBS"	Core Banking Solution
"CO"	Central Office
CVC	Central Vigilance Commission
DAM	Database Activity Monitoring
DC	Data Centre of the Bank which is located at Central Office, Belapur, Mumbai
DMZ	Demilitarized Zone
DNS	Domain Name Server
DRC	Disaster Recovery Centre which is located in Hyderabad
EMD	Earnest Money Deposit
EMS	Enterprise Management System
FPS	Flows Per Second
GbE/GigE/Gbps	Gigabit Per Second
GoI	Government of India

HA	High Availability
HDD	Hard Disk Drive
HO	Head Office
INR	Indian National Rupee
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
LAN	Local Area Network
Mbps	Megabits Per Second
MPLS	Multi-Protocol Label Switching
MTBF	Mean Time before Failure
NDA	Non-Disclosure Agreement
NOC	Network Operations Centre
NMS	Network Management System
OEM	Original Equipment Manufacturer
PO	Purchase Order
RFP	Request for Proposal
RMA	Return Material Authorization
RO	Regional Office
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SIEM	Security Information and event Management
SSD	Solid State Drive
SMTP	Simple Mail Transfer Protocol
SOAR	Security Orchestration Automation and Response
SoW	Scope of Work
SLA	Service Level Agreement

SPOC	Single Point of Contact
SSL	Secure Sockets Layer
T&C	Terms & Conditions
Tbps	Terabits per second
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TOR	Top of Rack
UAT	User Acceptance Test
VPN	Virtual Private Network
WAN	Wide Area Network
WAF	Web Application Firewall
ZO	Zonal Office

1. Invitation for Tender Offers

Central Bank of India, The Bank, a body corporate constituted under the Banking Companies (Acquisition and Transfer of Undertaking) Act 1970 having its Central Office at Chandermukhi, Nariman Point, Mumbai-400021 hereinafter called "Bank" and having 90 Regional Offices (RO), 12 Zonal Offices (ZO) and 4617 plus branches spread across India, intends for select a bidder for Supply, Installation and Maintenance of Cyber Security Solutions at Bank's DC, DRC, Branches and other offices

Bank invites online tender offers (Technical offer and Commercial offer) from eligible, reputed manufacturers and/or their authorized dealers for Supply, Installation and Maintenance of Cyber Security Solutions at Bank's DC, DRC, Branches and other offices.

The details are given below:

Date of RFP Issue	11/11/2024
Bid Security (EMD)	An amount of Rs.,1,60,00,000/- (Rupees One Crore Sixty Lacs Only) in the form of Bank Guarantee issued by a scheduled bank other than Central Bank of India for the entire period of Bid validity plus 3 months or by means of banker's cheque/ Account Payee Demand Draft /RTGS/NEFT in the account no.- 3287810289 of Central Bank of India (IFSC Code – CBIN0283154) with narration of Tender ref in favour of "Central Bank Of India" and payable at Mumbai/Navi Mumbai.
e-mail IDs for sending queries and Last Date for submission of queries	smit2infosec@centralbank.co.in, cminfosec@centralbank.co.in, smitpurchase@centralbank.co.in, latest by 20/11/2024 up to 16:00 hrs.
Date and time for Pre-Bid Meeting	22/11/2024 at 15:00hrs. (At Bank's CBD Belapur Address)
Last Date and Time submission of Bids Mode of bid submission	26/12/2024 up to 15:00 hrs.
Time & Date of Opening of technical bids	26/12/2024 at 15:30 hrs.
Mode of Submission	Government E Marketplace (GeM)
Response Types	1.Technical Bid plus Bid Security/EMD 2.Commercial Bid
Address for Communication	General Manager-IT Central Bank Of India Department Of IT (DIT),

	<p>Plot no-26, Sector-11, CBD Belapur, Navi Mumbai- 400614</p> <p>Mail address: smitpurchase@centralbank.co.in smit2infosec@centralbank.co.in cminfosec@centralbank.co.in</p>
Contact Telephone Numbers	022-67123583, 022- 67123669

For any clarification with respect to this RFP, the bidder may send their queries/suggestions, valuable inputs and proof of remittance of document cost or exemption certificate of MSE by email to the Bank. It may be noted that all queries, clarifications, questions etc., relating to this RFP, technical or otherwise, must be in writing only and should be sent to designated email ID within stipulated time as per Annexure 20. The Service Level Agreement with the successful bidder will be part and parcel of the RFP document. Therefore please note and ensure that all such queries are to be raised before bidding. Any query/ request for review of any clause of RFP/ SLA after the completion of bidding process shall not be entertained.

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

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

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

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

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

General Manager-IT
Central Bank of India, DIT,
CBD Belapur, Navi Mumbai-400614

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

This RFP is neither an agreement nor an offer and is only an invitation by Bank to the interested parties for submission of unconditional bids. The purpose of this RFP is to provide the bidder(s) with information to assist the formulation of their proposals. This RFP does not claim to contain all the information each bidder may require. Each bidder should conduct its own investigations and analysis

and should check the accuracy, reliability and completeness of the information in this RFP and where necessary obtain independent advice. Bank makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. Bank may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

2. Eligibility Criteria

The Bidder must fulfil following eligibility criteria:

#	Eligibility of the Bidder	Documents to be submitted	Compliance (Y/N)
1.	Bidder should be a Registered company under Indian Companies Act. 1956/2013 or LLP/Partnership firm and should have been in existence for a minimum period of 5 years in India, as on date of submission of RFP.	Copy of the Certificate of Incorporation issued by Registrar of Companies/Registrar of firms and full address of the registered office of the bidder	
2.	Bidder should be registered under G.S.T and/or tax registration in state where bidder has a registered office	Proof of registration with GSTIN	
3.	The bidder must have an average annual turnover in India of INR 500 crores per annum in the last three financial years (i.e., 2021-22, 2022-23, 2023-24), of individual company and not as group of companies*	Copy of Audited Balance Sheet and Copy of Certificate of the Chartered Accountant for the last three financial years (i.e., 2021-22, 2022-23, 2023-24)	
4.	The bidder should have made operating profits in at least two financial years out of last three financial years (i.e., 2021-22, 2022-23, 2023-24)* In case of operating loss, bidder will have to provide additional security amount of 20% of contract Value over and above 10% of regular Performance Bank Guarantee	Copy of Audited Balance Sheet and Copy of Certificate of the Chartered Accountant for the last three financial years (i.e., 2021-22, 2022-23, 2023-24)	
5.	The bidder should have a positive net worth in last three financial years (i.e., 2021-22, 2022-23, 2023-24)*	Copy of Audited Balance Sheet and Copy of Certificate of the Chartered Accountant for the last three financial years (i.e., 2021-22, 2022-23, 2023-24)	
6.	At the time of bidding, the Bidder should not have been blacklisted/debarred/ by any Govt. / IBA/RBI/PSU /PSE/ or Banks, Financial institutes for any reason or non-implementation/ delivery of the order. Self-declaration to that effect should be submitted along with the technical bid.	Submit the undertaking on Company's letter head	

#	Eligibility of the Bidder	Documents to be submitted	Compliance (Y/N)
7.	At the time of bidding, there should not have been any pending litigation or any legal dispute in the last five years, before any court of law between the Bidder or OEM and the Bank regarding supply of goods/services	Submit the undertaking self-declaration on Company's letter head	
8.	Bidder/OEM should not have <ul style="list-style-type: none"> NPA with any Bank /financial institutions in India Any case pending or otherwise, with any organization across the globe which affects the credibility of the Bidder in the opinion of Central Bank of India to service the needs of the Bank 	Submit self-declaration on Company's letter head.	
9.	Bidder should have service/support centre or should have arrangement for providing support in Mumbai and Hyderabad.	Submit the undertaking self-declaration on Bidder's letter head	
10.	If the bidder is from a country which shares a land border with India, the bidder should be registered with the Competent Authority	Certified copy of the registration certificate	
11.	Bidder should have a supplied, installed and maintained at least 4 out of the following solutions: <ol style="list-style-type: none"> Data Discovery & Classification File Upload Security Solution Attack Surface Management (ASM) Breach and Attack Simulation (BAS) along with Red Team Solution Phishing Simulation AD Security IT Governance, Risk & Compliance Decoy (Honey-pot) Mobile Device Management Secure Data Backup and Recovery (Ransomware Protection) Network Access Control (NAC) <p>in at least One Scheduled Commercial Banks/ "Govt/Public" Listed BFSI/ RBI/ NABARD/ NPCI in India.</p>	Reference Letter/ Purchase order of similar projects undertaken.	
OEM Eligibility Criteria			

#	Eligibility of the Bidder	Documents to be submitted	Compliance (Y/N)
12.	<p>For the proposed OEMs' solutions product series, minimum 7 out of the below solutions must have been implemented in at least One Scheduled Commercial Bank/ "Govt/Public" Listed BFSI/ RBI/ NABARD/ NPCI in India in last 5 years.</p> <ol style="list-style-type: none"> 1. Data Discovery & Classification 2. File Upload Security Solution 3. Attack Surface Management (ASM) 4. Breach and Attack Simulation (BAS) along with Red Team Solution 5. Phishing Simulation 6. AD Security 7. IT Governance, Risk & Compliance 8. Decoy (Honey-pot) 9. Mobile Device Management 10. Secure Data Backup and Recovery (Ransomware Protection) 11. Network Access Control (NAC) 	Reference Letter/ Purchase order of similar projects undertaken.	

***Note:** If case of unaudited Balance Sheet for FY 2023-24, Bidder needs to submit Provisional Balance Sheet along with copy of CA Certificate for FY 2023-24.

The bidder must submit only such document as evidence of any fact as required herein. The Bank, if required, may call for additional documents during the evaluation process and the bidder will be bound to provide the same. Bank reserves the right to verify references provided by the Bidder independently. Any decision of bank in this regard shall be final, conclusive, and binding up on the bidder. Bank may accept or reject an offer without assigning any reason whatsoever.

1. Bidders need to ensure compliance to all the eligibility criteria points.
2. In-case of corporate restructuring the earlier entity's incorporation certificate, financial statements, Credentials, etc. may be considered.
3. In case of business transfer where Bidder has acquired a Business from an entity ("Seller"), work experience credentials of the Seller in relation to the acquired business may be considered.
4. Bidder must provide credential letter or successful installation sign off document.
5. Scheduled Commercial Bank does not include Payments Bank, Cooperative Banks or RRBs.
6. While submitting the bid, the Bidder is required to comply with inter alia the following CVC guidelines detailed in Circular No. 03/01/12 (No.12-02-6 CTE/SPI (I) 2 / 161730 dated 13.01.2012): 'Commission has decided that in all cases of procurement, the following guidelines may be followed:

- a. *In RFP, either the Indian agent on behalf of the Bidder/OEM or Bidder/OEM itself can bid but both cannot bid simultaneously for the same item/product in the same RFP. The reference of 'item/product' in the CVC guidelines refer to 'the final solution that bidders will deliver to the customer.*
- b. *If an agent submits bid on behalf of the Bidder /OEM, the same agent shall not submit a bid on behalf of another Bidder /OEM in the same RFP for the same item/product.*

3. EMD / Bid Security

An amount of ₹ 1,60,00,000/- (Rupees One Crore Sixty Lacs Only) in the form of Bank Guarantee issued by a scheduled bank other than Central Bank of India for the entire period of Bid validity plus 3 months or by means of Account Payee Demand Draft / banker's cheque /RTGS/NEFT in the account no.-3287810289 of Central Bank of India (IFSC Code – CBIN0283154) with narration Tender ref in favour of "Central Bank Of India" and payable at Mumbai/Navi Mumbai.

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

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

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

The EMD / Bid Security will be refunded to The Successful Bidder, only after furnishing an unconditional and irrevocable Performance Bank Guarantee (PBG) as per Sr no.4

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

4. Performance Bank Guarantee

- i. As mentioned above, the Successful Bidder will furnish an unconditional and irrevocable Performance Bank Guarantee (PBG) from scheduled commercial Bank other than Central Bank of India, in the format given by the Bank in Annexure 11, for 10% of the total project cost valid for 66 months, (5 years for total project period plus 6 months for claim period) validity of PBG starting from its date of issuance. The PBG shall be submitted within 21 days of the PO acceptance by the Bidder.
- ii. The PBG so applicable must be duly accompanied by a forwarding letter issued by the issuing bank on the letterhead of the issuing bank. Such forwarding letter shall state that the PBG has been signed by the lawfully constituted authority legally competent to sign and execute such legal instruments. The executor (BG issuing Bank Authorities) is required to mention the Power of

Attorney number and date of execution in his / her favour with authorization to sign the documents.

- iii. Each page of the PBG must bear the signature and seal of the PBG issuing Bank and PBG number.
- iv. In the event of the Successful Bidder being unable to service the contract for whatever reason, Bank may provide a cure period of 30 days and thereafter invoke the PBG, if the bidder is unable to service the contract for whatever reason.
- v. In the event of delays by Successful Bidder in AMC support, service beyond the schedules given in the RFP, the Bank may provide a cure period of 30 days and thereafter invoke the PBG, if required.
- vi. Notwithstanding and without prejudice to any rights whatsoever of the Bank under the contract in the matter, the proceeds of the PBG shall be payable to Bank as compensation by the Successful Bidder for its failure to complete its obligations under the contract, indicating the contractual obligation(s) for which the Successful Bidder is in default.
- vii. The Bank shall also be entitled to make recoveries from the Successful Bidder's bills or any other amount due to him, the equivalent value of any payment made to him by the bank due to inadvertence, error, collusion, misconstruction or misstatement.
- viii. The PBG may be discharged / returned by Bank upon being satisfied that there has been due performance of the obligations of the Successful Bidder under the contract. However, no interest shall be payable on the PBG.
- ix. For release of remaining 10% of Hardware and Software component of the payment terms Bank Guarantee equivalent to 10% of the deliverable is required to be submitted in addition to the above PBG.

5. Cost of Bidding

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

6. Manufacturer's Authorization Form

Bidders must submit a letter of authority from their manufacturers in Annexure 8 that they have been authorized to quote OEM Product.

7. Scope of Work

Central Bank of India intends to procure Cyber Security Solutions and associated Hardware including Storage to meet Banks future business requirements and to appoint a proven & experienced Bidder to Supply, Install/Implement, Configure and Integrate new Cyber Security Solutions into the existing SIEM and SOAR Solution.

- Data Centre (DC) of the Bank is in Navi Mumbai. Disaster Recovery Centre (DRC) is located at Hyderabad.
- The Bank has envisaged the procurement of New Cyber Security Solutions and associated hardware, details of the same have been provided in Annexure 1: Bill of Materials. The Bidder is required to quote the Cyber Security Solutions in compliance to the Technical Specifications given in Annexure 2: Technical Specifications.
- Procurement of the Cyber Security Solutions and associated hardware mentioned in the RFP will be at Bank's discretion and Bank may not procure all the items mentioned in the RFP. Also, Bank may ask for staggered delivery of some of the Cyber Security Solutions and associated hardware mentioned in the RFP. Details of the same would be shared with the successful Bidder at a later stage.
- Bidder must provide the details of each individual proposed Cyber Security Solutions and associated hardware along with the Hardware & Software proposed, in Annexure 1: Bill of Materials.
- Whatever is required for the successful implementation of the proposed cybersecurity solutions, such as x86 based Hardware including any OS, VMs and Load Balancer etc., the Bidders has to provide the same.
- Also, bidder is required to provide the necessary co-hosting details for the proposed solutions in terms of space, power and cooling requirement. However, the same shall be provided by the Bank.
- Bidder is also required to provide the number of ethernet ports (with speed) required for all the Proposed Solutions. However, the same shall be provided by the Bank.
- All the services/solutions offered should be modular, scalable, and should be able to meet Bank's requirements during the period of contract.
- All the services/solutions in scope needs to be designed and implemented with adequate redundancy and fault tolerance to ensure compliance with Service Levels for uptime as outlined in this RFP.
- It should be ensured that during installation/implementation and during operations of the security solutions; none of the existing infrastructure/ business of the Bank should be impacted.
- Bidder is also required to carry out activities given in the following table

Sr. No.	Activity	Remarks
1.	Physical delivery of Cyber Security Solutions and associated hardware	Bidder must supply and deliver the Security Solutions and associated hardware mentioned in Annexure 1: Bill of Materials at the Bank's site and in compliance to the Annexure 2 - Technical Specifications given in the RFP
2.	Installation, configuration & implementation of Cyber	OEM / OEM Authorised Partner is required to install, configure and implement the Cyber Security Solutions and

	<p>Security Solutions and associated hardware to suit the requirements.</p>	<p>associated hardware provided by the OEM/s. Thus, OEM / OEM Authorised Partner is required to unpack, assemble, mount, and boot the solutions/equipment and install the necessary service packs, patches, and fixes to the Operating System, set up and configure the solution. Compatibility issues of subsystems with OS, respective drivers, firmware, any other cards to be installed, if required, are to be resolved by Bidder. OEM / OEM Authorised Partner is required to ensure the successful implementation of the Cybersecurity Solutions part of this RFP.</p> <p>Bidder should supply, install, configure, integrate the Cyber Security Solutions and associated hardware. Bank's existing System Integrator and the Bank will conduct the acceptance test and verify that the installation complies with the configuration and relevant setting provided by the Bank's existing System Integrator.</p> <p>In case of new solution proposed for the existing solution, in such case bidder is required to do migration of data to the new proposed solution. The sole responsibility of migration lies with the bidder.</p>
<p>3.</p>	<p>Provide warranty and AMC/ATS support for the tenure of the contract</p>	<p>Bidder will be responsible to provide the following services during the Contract period</p> <ul style="list-style-type: none"> • Onsite comprehensive warranty from OEM, • AMC/ATS from the OEM • Arrange back-to-back support from the respective OEMs. Bidder is required to submit proof (Certificate / mail from oem / letter etc) of back-to-back support from OEMs. <p>In Case of RMA, it is bidder responsibility to replace the equipment as per SLA and to return the faulty equipment to the OEM warehouse at no extra cost to the Bank during the tenure of the contract.</p>
<p>4.</p>	<p>Complete Migration of Data and Policies from existing solutions to new solutions (if applicable)</p>	<p>Bidder will be responsible to ensure complete migration of data and policy from existing solutions of IT Governance, Risk and Compliance (GRC), Decoy (Honeypot), NAC and Mobile Device Management (MDM) to the newly proposed solutions.</p> <p>Complete Migration from existing to new solutions</p> <p>The sole responsibility of migration lies with the bidder.</p>

- Considering the nature of the Security Solutions, it may happen that the bidder may propose a solution suite consisting of multiple features, functionalities suiting to the RFP requirements

and in compliance of RBI cyber security circulars. The bidder shall provide the solutions with all such features (over and above to technical specifications) without any additional cost to the Bank. All the available functionalities should be available to the Bank. The bidders shall include all necessary expenses in complete cost of the respective line items of the solution in Annexure – 1: Bill of Material. All costs shall be included in the line items only.

- The solutions should include all components and subcomponents like software licenses, accessories, and the bidder should supply any other components that is required for the successful installation and commissioning of the solutions that are part of this RFP (if not specified in the Bill of Materials) at no additional cost to the Bank. The bidder should consider all the components required for the successful installation and commissioning of the solutions that are part of this RFP while quoting price for the solutions.
- It is the bidder's responsibility to ensure complete migration of data and policy from the existing solutions of IT Governance, Risk and Compliance (GRC), Decoy (Honeytrap) and Mobile Device Management (MDM) to the newly proposed solutions as per Bank's requirement.
- Bidder to ensure that the complete installation and commissioning of all the solutions part of this RFP to be done by the respective OEMs or by OEM Authorised Partners till the successful implementation of the respective solutions. OEMs to provide the certification of authorization for their respective partners.
- After the successful implementation of the solutions by the OEM's, Bidder and OEM to ensure complete handover process is performed from the OEMs to the Bidder team including all documentation.
- The Bidder must Supply, Install/Implement, Configure and Integrate the Cyber Security Solutions and associated hardware into the existing SIEM, PIM, any other such security Solution. Bidder must also provide subsequent comprehensive on-site warranty/AMC/ATS for the proposed Cyber Security Solutions (Hardware, Software, etc.) and associated hardware as per the Bill of Materials shared by the Bank. The delivery plan must be synchronized with the project delivery timelines of the Bank.
- Bidder is also required to provide skilled resources that may be required for the successful completion of the project.
- The Cybersecurity Solutions Hardware should be provided with 3 years of on-site comprehensive warranty which will start from the date of acceptance of Cyber Security solution. Subsequently, Bidder shall provide the AMC support for the remaining two Years post warranty period.
 - The warranty will start only after acceptance of Installation.
 - The Bidder has to submit proof for back-to-back agreement with the Hardware and Software OEM.
- The Cybersecurity Solutions Software should be provided with 1 years of on-site comprehensive warranty which will start from the date of acceptance of Cyber Security solution. Subsequently, Bidder shall provide the ATS support for the remaining four Years post warranty period.
- Bidder is required to co-ordinate with Bank's existing System Integrator for monitoring and troubleshooting for support, throughout the tenure of the contract.
- Bank has option to extend contract period for additional 2 years at the same prices quoted for AMC/ATS of 5th year for in scope components of this RFP.

- The bidder should have a 24x7x365 days support contact center in India in order to log the calls. The contact center numbers should be provided to the Bank along with the escalation matrix mentioning the contact person's name, number and designation in the company
- The bidder should provide 24*7 support for any kind of issue in functionality/performance/integration of the platform during the entire tenure of contract. In case, the issue is not resolved for more than 8 hours, support personnel has to escalate as per the escalation matrix. The bidder shall provide the details of support team and escalation matrix for immediate assistance to bank's team for any issue.
- No external remote access will be provided for any issues. Bidders are required to provide onsite resources.
- OEM should be present in India for more than 3 years and preferably should be having support centre in India.
- The solution deployed should be compliant with Bank's IS, IT and Cyber Security policies, internal guidelines, regulatory requirements and countrywide regulations and laws.
- The Bidder would be responsible for supply, installation, testing, commissioning, configuring, Operation & Maintenance of the solutions, warranty and AMC of licenses (hardware, software, middleware supplied) as part of this RFP for a period of Five (5) years.
- The contract will be for a period of FIVE years from the date of Go-live.
- During the tenure of the contract, all upgrades or requirements in hardware, software, licensing, implementation of upgrades/patches/version changes etc., due to whatsoever reason including but not limited to EOL or EQS, would be done by the bidder without any additional cost to the bank.
- If a solution fails to meet the technical requirements of RFP during the implementation/before sign-off phase, Bank reserves the right to reject the solution with no cost to the Bank and recover all payments made for that solution. However, in such cases the bidder may offer alternate solution to the Bank which fulfils technical requirements of the RFP with no extra cost to the Bank.
- If during the contract period, the solution is not performing as per specifications in this RFP, bidder shall upgrade/enhance the devices or place additional devices and reconfigure the system without any extra cost to the bank till the required performance is achieved.
- All the Cyber Security Solution must be tightly integrated with SIEM, SOAR, UEBA,PIM,IT Service Desk (Call Logging System), any other such solution.
- The Bidder is required to Integrate all Cyber Security solutions and associated hardware with SOAR, SIEM, PIM and existing ticketing Solution
- All Solutions must be implemented by OEM / OEM authorized service Partner only. In case of OEM authorized partner, valid document should be provided by the OEM for authorising the partner.
- Training – overall for 10 participants for minimum 1 week on all the solutions part of this RFP; Training from OEM / OEM authorized service Partner. Bidder has to provide the same at no additional cost to the Bank.
- **OEM's Assessments Reports**
Bidders must ensure that all the above solutions are being assessed by the respective OEM's of the proposed products
 - i. Respective OEMs to check that the proposed functionality that are part of RFP including technical specifications are working properly
 - ii. Assessment is to be performed twice in a year post successful installation for year one and performed once in year for remaining years, during the period of contract.

- iii. OEM to submit and present the reports to bank. In case of any findings, bidder is required to bridge those gaps as per the recommendations of the OEMs during the tenure of contract, at no additional cost to the bank.

7.1 Detailed Scope of Work

The Bidder is required to supply, install, integrate, maintain, and provide AMC for the following (Cyber Security Solutions and associated hardware mentioned in subsection) solutions for the period of contract at Bank's offices. In case of any compatibility issue arises between the proposed solutions/appliance and existing SIEM setup during implementation or within 3 months of installation signoff, then the successful bidder is required to replace such solutions/appliances, with the compatible one, at no additional cost to the bank within 4 weeks of the issue being intimated by Bank.

- The proposed solution should be tightly integrated with all the existing tools / setup and new infrastructure /Assets of the Bank. The selected bidder should implement and maintain these Cyber Security Solutions and associated hardware for Bank's Infrastructure for a period of contract.
- The selected bidder should provide detailed solution document, project implementation/migration plan, new architecture diagram (HLD and LLD) and provision for hosting the proposed solution.
- For the solutions in scope, the Bidder is required to propose appliance, Hardware or software or a combination of hardware and software to meet the individual requirements put forward by the Bank for the respective solutions. Bidder is required to Design, size, supply, install & maintain the required security solutions for the period of contract.
- Bidder is required to Supply, Install/Implement, Configure and Maintain the following Cyber Security Solutions and associated hardware for the period of contract -
 1. Data Discovery & Classification
 2. File Upload Security
 3. Attack Surface Management (ASM)
 4. Breach and Attack Simulation (BAS) along with Red Team Solution
 5. Phishing Simulation
 6. AD Security
 7. IT Governance, Risk & Compliance
 8. Decoy (Honeypot)
 9. Mobile Device Management
 10. Secure Data Backup and Recovery (Ransomware Protection)
 11. Network Access Control (NAC)
- In case of refresh items, that are part of the bill of material, wherein the bidder is proposing new solutions for the existing solutions implemented at Bank, the bidder is required to perform complete migration of all the data from the existing solution to the new solution.
- Bidder is required to refer to tab "Solutions Sizing" in Annexure 2 – Minimum Technical Specifications for guidelines for sizing and licensing of the above solutions.

7.1.1 Data Discovery & Classification

- The bidder is required to Supply, install and Maintain Data Discovery & Classification solutions at Bank for the period of contract. The proposed solution is required to meet the technical specifications and bill of material s given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.
- The proposed data discovery and classification solution should be tightly integrated with the existing DLP Solution.
- Solution should improve Data Loss Prevention Accuracy and should offer seamless integration with existing DLP Solution. DLP solution should leverage the use of this tool.
- Solution should provide visibility of critical data in the Bank.
- Solution should raise security awareness among end users and educate them on data handling.
- Proposed Solution should enable to establish a policy-driven foundation that helps to identify and classify sensitive data at creation, in motion, or at rest and apply the right security policy to protect it. Solution should work with email and office applications as a part of user's day-to-day workflow for identification and classification of mails and documents.
- Policy engine of proposed solution should provide granular options to build policies based on various conditions like AD user, department, file content, file attributes, recipients, location, printer, etc., and these policies shall be triggered based on different Events like creating a new file, opening an existing file or emailing a document, etc.
- Solution should classify other file/file types on Windows OS and the functionality is part of the same endpoint agent. For all other files, Solution must classify the file based on file attributes (file location, file size, file name or based on logged in user etc.)
- Solution should provide a breadth of tools that enable customers to detect sensitive data with Regex, Smart Regex, Categorization using Machine Learning (ML) and natural language processing capabilities do detect PCI, PII, etc., The solution should also be configured to detect specific keywords that may be critical for the Bank.
- Solution must capture time sensitivity of a document. Example - Financial statement needs to be classified confidential until public release on 1st April and post that it should be classified as public.
- The Bidder shall involve their resources in Data Collection, Policy/Rule Creation/Fine-Tuning, Policy/Rule Enforcement and Incident Management Support.
- The tool shall be capable to perform the data classification as per Bank's data classification policy
- Bidder shall conduct awareness programs among end users as and when Bank requires.
- Sizing Guidelines for all the solutions can be found in Annexure 2 - Minimum Technical Specifications, in the sub titles "Solutions Sizing".
- Data Discovery and Classification solution should provide actionable reports, such as but not limited to below mentioned reports:
 - 1) Data Inventory Reports - The Data Discovery and Classification solution should provide comprehensive list of data assets across the Bank, show where sensitive data resides, identify data formats (structured, unstructured, semi-structured) and provide information on data size and growth.

- 2) Data Classification Reports - The Data Discovery and Classification solution should classify data based on sensitivity levels, identify data owners and custodians, show who has access to sensitive data and analyse how data is being used.

7.1.2 File Upload Security

- The bidder is required to Supply, Install and Maintain “File Upload Security” solutions at Bank for the period of contract. The proposed solution is required to meet the technical specifications and bill of material given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.
- Bidder is required to configure File Upload Security at DC as Primary and at Disaster Recovery site as secondary, having high availability across DC and DRC. In case of DR Drill or DC fails, File Upload Security at DRC should act as Primary
- The proposed File Upload Security solution should proactively prevent cyber threats from entering a network through files. It should act as a pre-emptive shield against malicious content hidden within documents, emails, or other downloadable files.
- The proposed File Upload Security solution should Disarm Malicious Content and Preserving Functionality.
- The proposed File Upload Security solution should Enhanced Protection, Zero-Day Threat Protection and Improved User Experience.
- The file upload / download sources are
 1. Email (/attachment)
 2. WAF
 3. SFTP and
 4. API
 5. Other channels in Bank
- Sizing Guidelines for File Upload Security can be found in Annexure 2 - Minimum Technical Specifications, in the sub tab titles "Solutions Sizing".
- File Upload Security solution should provide actionable reports, such as but not limited to below mentioned reports:
 1. Threat Detection Reports – The File Upload Security solution should provide information on identification of files containing malware, viruses, or other threats, identification of files containing exploits or vulnerabilities.
 2. File Analysis Reports - The File Upload Security solution should provide identification of file types and formats scanned, detection of abnormally large or small files, identification of sensitive data within files, information of embedded objects/scripts and verification of file format integrity.
 3. Incident response reports - The File Upload Security solution should be able provide detailed information about specific file , it's object ,properties and behavior if found malicious or suspicious.

7.1.3 Attack Surface Management (ASM)

- The bidder is required to Supply, Install and Maintain “Attack Surface Management” solutions at Bank for the period of contract. The proposed solution is required to meet the technical specifications and bill of material given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.

- Bidder is required to configure ASM solution at DC as Primary and at Disaster Recovery site as secondary, having high availability across DC and DRC. In case of DR Drill or DC fails, ASM Solution at DRC should act as Primary
- The proposed Attack Surface Management (ASM) solution should reduce the risk of cyberattacks by providing a comprehensive view of your organization's attack surface and proactively addressing vulnerabilities.
- The proposed ASM should provide visibility of attack surfaces as all the potential entry points for a hacker. This should include devices, applications, data, systems, and even your online presence. ASM should continuously discover and inventory all IT Bank's assets, both internal and external to your network.
- The proposed ASM should provide vulnerability assessment in terms of identifying weaknesses within those assets. This might involve outdated software, misconfigured systems, or weak passwords. By pinpointing vulnerabilities, Bank's / SI's IT team should prioritize patching and remediation efforts.
- The proposed ASM solution should reduce attack points; by removing unused systems, hardening configurations, or segmenting your network to limit access to critical resources.
- The proposed ASM should support proactive threat detection by analysing how attackers might exploit those weaknesses. By simulating attacker behavior (ethical hacking), ASM should identify potential attack vectors and take steps to mitigate them before they're used in a real attack.
- The ASM Solution should be tightly integrated with the Bank's existing solutions, but not limited to, such as Antivirus, EDR, HIPS, VA Scanner, Active Directory, NIPS, NGFW, Sandboxing, Anti APT or any other solution that bank currently has or will procure in the future.
- The proposed ASM solution should tightly integrate with existing security tools (SIEM, SOAR) tools.
- Sizing Guidelines for Attack Surface Management can be found in Annexure 2 - Minimum Technical Specifications, in the subtab titles "Solutions Sizing".
- Attack Surface Management solution should provide actionable reports, such as but not limited to below mentioned reports:
 1. Asset Inventory Reports – The Attack Surface Management solution should identify all assets exposed to the internet, categorize assets based on criticality and sensitivity, assign responsibility for asset management and detect unauthorized IT resources.
 2. Vulnerability Assessment Reports - The Attack Surface Management solution should identify vulnerabilities in assets, rank vulnerabilities based on risk, tracks patch management status and evaluate the likelihood of successful exploitation.
 3. Risk Assessment Reports – The Attack Surface Management solution should quantify the potential impact of vulnerabilities, correlate vulnerabilities with known threats and assess the potential impact on business operations
 4. Exposure Reports - The Attack Surface Management solution should list exposed services and their vulnerabilities, identify all domains and subdomains, evaluate the risk posed by vendors and partners
 5. Remediation Reports - The Attack Surface Management solution should track progress in addressing vulnerabilities and support incident response strategies.
 6. Compliance Reports - The Attack Surface Management solution should provide documentation for security audits.

7.1.4 Breach and Attack Simulation (BAS) with Red team solution

- The bidder is required to Supply, Install and Maintain “Breach and Attack Simulation (BAS) with Red team solution” solutions at Bank for the period of contract. The proposed solution is required to meet the technical specifications and bill of material given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.
- Bidder is required to configure Breach and Attack Simulation (BAS) with Red team solution at DC as Primary and at Disaster Recovery site as secondary, having high availability across DC and DRC. In case of DR Drill or DC fails, Breach and Attack Simulation (BAS) with Red team solution at DRC should act as Primary
- The Bidder should Supply, Installation, commissioning, integration, maintenance, and operations of the BAS solution as per the required technical specifications, in both DC & DR
- The Bidder should assist the Bank in identification of the zones to deploy BAS agents along with required prerequisites for connectivity between the attacker machine and BAS agents, and between attacker machines and Threat library
- The Bidder should activate all Attack Modules across all Threat Vectors - Network, URL Filtering, Endpoint, WAF, Email and Data Exfiltration - to simulate real-world attacks and proactively test the Bank's defences in a risk-free environment using pure 'simulation' approach, without causing any harm to the Bank's production environment
- The Bidder should integrate all relevant technology solution components and integrate the BAS platform with the existing SOC Platform of the Bank. Configuration and fine tuning of the platform on continuous basis
- The Bidder should assist the Bank to create and execute various threat campaigns on Endpoints, Servers, Email, Perimeter devices like Firewall, IDS, IPS, etc. as prescribed by the Bank. This should include campaigns for Ransomware, Emerging Threats, Attacks targeted towards Banking & Financial Institutions, Campaigns from BFSI-focused APT Groups, etc.
- The Bidder should provide guidelines to determine the critical threat campaigns / attacks that should be simulated in the Bank's environment. Update the Bank about new threat campaigns / attacks that are added to their threat library on a regular basis
- The Bidder should provide vendor-specific mitigation recommendations for all supported technologies deployed in the Bank. Assist the bank's security operations team in implementation of vendor-specific mitigation recommendations (signatures) for prevention controls (like NGFW, IPS, WAF) TO improve the Bank's security posture on a regular basis.
- The Bidder should integration of the BAS platform with the SIEM, SOAR, EDR, XDR Solution for detection visibility, understanding detection capabilities post execution of threat campaigns, assist in implementation of mitigation recommendations (missing logs and alerts) for detection controls
- The Bidder should use the 'Assumed Breach Approach' to perform Automated Red Teaming on the Bank's systems with pre-specified goals to identify the real attack paths (not all hypothetically possible)
- The Bidder should continuously discover attack paths that lead to the Bank's critical assets, enabling full visibility into the Bank's security posture
- The Bidder should discover hidden elements throughout the Bank's network that enable environment enumeration, lateral movement and privilege escalation
- The Bidder should conduct two health-checks every year to check BAS platform as per best practices and/or recommended configuration and provide the health check document.

Conduct the implementation of upgrades/ patches/ version changes during the tenure of the contract

- The Bidder should assist the Bank in the preparation of monthly/quarterly reports which include threat campaigns executed, security posture rating, prevention and detection scores, MITRE ATT&CK mapping, security posture improvement
- The Bidder should enable the Bank's security team members with Red Teaming and Blue Teaming oriented cybersecurity trainings without any additional charge
- Breach and Attack Simulation solution should provide actionable reports, such as but not limited to below mentioned reports:
 1. Threat Simulation Reports - The BAS solution should simulate attacks based on real-world threat actor tactics, techniques, and procedures (TTPs), should evaluate the ability of Bank's security tools to detect simulated attacks, and assess the effectiveness of Bank's incident response plan.
 2. Security Control Effectiveness Reports - The BAS solution should evaluate the effectiveness of security controls in preventing or detecting attacks, should highlight areas where security controls are lacking, and should suggest improvements to enhance control efficiency.
 3. Attack Path Analysis Reports - The BAS solution should be able to visualize how an attacker could move laterally within the network, identify sensitive data exposed to potential attackers and recommend steps to block attack paths.
 4. Executive Summaries - The BAS Solution should provide high-level overview which summarizes key findings and recommendations.
- A red teaming solution should provide a comprehensive assessment report of the Bank's security posture by simulating real-world attacks, which should help Bank's team in understanding the Banks's vulnerability landscape and prioritizing remediation efforts.

7.1.5 Phishing Simulation

- The bidder is required to Supply, Install, configure and maintain "Phishing Simulation" solutions at Bank for the period of contract. The proposed solution is required to meet the technical specifications and bill of material given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.
- Bidder is required to configure Phishing Simulation solution at DC as Primary and at Disaster Recovery site as secondary, having high availability across DC and DRC. In case of DR Drill or DC fails, Phishing Simulation Solution at DRC should act as Primary
- The proposed Phishing simulations should test your Bank's employees' ability to identify and respond to phishing attacks. These simulations mimic real-world phishing emails, text messages, or even phone calls in a controlled environment.
- The proposed phishing simulation solution should support features such as Raising Security Awareness, Identifying Susceptible Employees, Improving Overall Security Posture, and Testing Security Controls.
- By conducting phishing simulations regularly, it should significantly improve Bank's ability to defend against phishing attacks, a common and evolving cyber threat.
- The platform shall facilitate creation of phishing campaigns including QR code phishing which can be customized by bank.
- The bidder should provide services for conducting simulated phishing, vishing and smishing exercises to improve cyber security awareness of bank staff, vendor employees, employees in

Overseas branches, employees in Bank's subsidiaries and Board of Directors etc. The resource for conducting the simulated phishing, vishing and smishing exercises shall be deployed in Hyderabad/Mumbai and shall be responsible to complete the exercises as per bank's requirement and submit the report.

- The bidder should provide daily, weekly, monthly status reports or as and when needed by the Bank.
- The bidder should be responsible for delivering social engineering exercises related to simulated vishing and smishing for the tenure of contract.
- The bidder should be capable of performing vishing exercises in both automated and manual methods. The automated approach shall support scalability in conducting vishing campaigns through Bidder's infrastructure/gateway.
- Sizing Guidelines for Phishing Simulation can be found in Annexure 2 - Minimum Technical Specifications, in the subtab titles "Solutions Sizing".
- The Phishing Simulation solution should provide actionable reports, such as but not limited to below mentioned reports:
 1. Campaign Performance Reports – The Phishing Simulation solution should report on the percentage of users who clicked on phishing links, percentage of users who opened phishing emails, should identify Bank's departments with higher susceptibility, average time taken by users to report a phishing email and measure the success of the phishing simulation.
 2. User Behavior Reports - The Phishing Simulation solution should report individual user performance and identify users who consistently fall for phishing attempts.
 3. Training Effectiveness Reports - The Phishing Simulation solution should measure the effectiveness of security awareness training, should tracks changes in user behavior after training.
- Threat Intelligence Reports - The Phishing Simulation solutions should update threat vectors/Library with emerging phishing tactics and techniques and help in Identification of potential threat actors targeting the Bank.

7.1.6 AD Security

- The bidder is required to Supply, Install, configure and maintain "AD Security" solutions at Bank for the period of contract. The proposed solution is required to meet the technical specifications and bill of material given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.
- Bidder is required to configure AD Security solution at DC as Primary and at Disaster Recovery site as secondary, having high availability across DC and DRC. In case of DR Drill or DC fails, AD Security Solution at DRC should act as Primary
- AD Security solution should enhance Active Directory (AD) defences by enforcing access controls, monitoring privileged accounts, and detecting anomalous activities. The proposed solution should protect against insider threats and external attacks, ensuring the integrity and confidentiality of AD infrastructure critical to Bank's operations and data security.
- The bidder is required to Supply, Install, configure and maintain "AD Security" solutions at Bank for the period of contract. The proposed solution is required to meet the technical specifications and bill of material given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.

- The proposed AD Security solution should protect the critical Active Directory (AD) services that manage identities and access throughout a network, that is name a few, control System Access, should protect Credentials and also should reduce the attack surface.
- The Proposed AD Security Solution should support breadth of capabilities to audit, monitor, harden, and secure AD.
- There are several steps Bank can take to improve their AD security. The bank should follow best practices such as “use Strong Passwords”, “Enforce complex passwords, Least Privilege, Regular Monitoring and finally software and finally Keep Software Updated.
- The proposed AD Security Solution should support following features such as:
 1. Audit Accounts & Privileges
 2. Attack Path Discovery
 3. Real-Time Protection and
 4. AD Backup & Recovery
- Sizing Guidelines for AD Security can be found in Annexure 2 - Minimum Technical Specifications, in the sub tab titles "Solutions Sizing".
- The AD Security solution should provide actionable reports, such as but not limited to below mentioned reports:
 1. User-Related Reports – The AD Security Solution should identify users who haven't logged in for a specified period, list users who have been locked out, show accounts with expiring or expired passwords, and identify users with administrative privileges, display groups memberships.
 2. Group-Related Reports – The AD Security solution should list members of specific groups, show group memberships within groups.
 3. Security-Related Reports – The AD Security Solution should display security events and actions, show permissions and access rights for users and groups, identify potential security weaknesses.

7.1.7 IT Governance, Risk and Compliance (GRC)

- Currently Bank is using IT Governance, Risk and Compliance Solution.
- The bidder is required to Supply, Install, configure and maintain "IT Governance, Risk and Compliance" solutions at Bank for the period of contract. The proposed solution is required to meet the technical specifications and bill of material given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.
- Bidder is required to configure IT Governance, Risk and Compliance solution at DC as Primary and at Disaster Recovery site as secondary, having high availability across DC and DRC. In case of DR Drill or DC fails, IT Governance, Risk and Compliance Solution at DRC should act as Primary
- 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
 - Streamline basic audit processes with intuitive documentation
 - Increase audit efficiency with better planning and reporting
 - 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:
 - Align risk management with business value drivers
 - Gain insight into how risks occur
 - Act on emerging risks and opportunities
 8. Scalable (capable of implementing one module/service at a time and adding users as needed).
- Bidder should integrate the proposed IT security GRC solution with the Bank's existing policies
 - Bidder needs to ensure all existing compliance requirements of the Bank and other Banking regulatory bodies are incorporated
 - Bidder is responsible for migration of all the data and policies from existing solution to the proposed solution.
 - Sizing Guidelines for IT Governance, Risk and Compliance can be found in Annexure 2 - Minimum Technical Specifications, in the sub tab titles "Solutions Sizing".
 - The IT Governance, Risk and Compliance solution should provide actionable reports, such as but not limited to below mentioned reports:
 1. Governance Reports - The IT GRC Solution should monitor adherence to organizational policies, track stakeholder engagement and satisfaction and measure the effectiveness of governance initiatives.
 2. 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.
 3. 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.
 4. Audit Reports – The IT GRC Solution should outline audit objectives and scope, document audit findings and recommendations and track progress on audit recommendations.

7.1.8 Decoy (Honeytrap)

- Currently Bank is using Decoy (Honeytrap) Solution.
- The bidder is required to Supply, Install, configure and maintain "Decoy (Honeytrap)" solutions at Bank for the period of contract. The proposed solution is required to meet the technical

specifications and bill of material given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.

- Bidder is required to configure Decoy (Honeytrap) solution at DC as Primary and at Disaster Recovery site as secondary, having high availability across DC and DRC. In case of DR Drill or DC fails, Decoy (Honeytrap) Solution at DRC should act as Primary
1. The proposed Honey Pot solution should be able to address the following key areas but not limited:
 1. Effectively create a replica copy of the Banks' existing internet-facing landscape
 2. Hacking incentive of the proposed decoy ecosystem should be as equivalent to present exposed incentive of the Bank
 3. The intended solution must safeguard the Bank against a target Reconnaissance attack, Lateral movement, Privilege Escalation, ransom ware and also act as a layer of defense for attacks based on new vulnerabilities, data theft and zero-day attacks
 4. Should provide real time Alerts
 2. The solution should be able to integrate with the Active Directory
The Bidder is expected to implement the solution across the Banks' internet facing landscape and any other critical service as deemed by the Bank.
The bidder must integrate the honeypot solution with SIEM to generate alerts for any violations.
 3. The primary responsibility of integration of solutions with existing SIEM lies with the Bidder selected through this RFP. The Bank shall provide adequate support to the Bidder for the purpose of integration.
 4. Bidder should ensure the maintenance of the solution and provision of logs in integration with the SIEM for review with the Bank.
 5. 24*7 monitoring of all the websites and services under the architecture of Honeytrap with no exceptions
 6. Bidder is responsible for migration of all the data and policies from existing solution to the proposed solution.
 7. Sizing Guidelines for Decoy (Honeytrap) can be found in Annexure 2 - Minimum Technical Specifications, in the subtab titles "Solutions Sizing".
 8. The proposed Decoy solution should provide a detailed view, such as but not limited to the below-mentioned telemetry:
 1. Attacker Behavior telemetry - The Decoy Solution should provide detailed information about the attacker, including IP address, geolocation, and attack techniques, identify common attack patterns and trends, analyze attack frequency over time and identify primary attack vectors used (e.g. Endpoint, web, network).
 2. Threat Intelligence - The Decoy Solution should detect security threats that might become initial attack vectors, leading to data breaches. It should also detect the well-known vulnerabilities and should have dynamic-ness to engage attackers.
 3. System Compromise - The Decoy Solution should detect signs of system compromise, identify attempts to steal data and detect attacker movement within the network
 4. Incident Response Reports - The Decoy Solution should provide a detailed chronology of attack events, documentation of mitigation steps and Automatic containment with 3rd party vendors

7.1.9 Mobile Device Management (MDM)

- Currently Bank is using Mobile Device Management Solution.
- The bidder is required to Supply, Install, configure and Maintain "Mobile Device Management" solutions at Bank for the period of contract. The proposed solution is required to meet the

technical specifications and bill of material given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.

- Bidder is required to configure Mobile Device Management solution at DC as Primary and at Disaster Recovery site as secondary, having high availability across DC and DRC. In case of DR Drill or DC fails, Mobile Device Management Solution at DRC should act as Primary
- The following elements are all required to construct a complete, end-to-end mobility solution.
- Mobile devices, such as notebook PCs, tablet PCs, personal digital assistants (PDAs), Smart Phones, data and Internet services Infrastructure to support the application, especially next generation (4G) wireless networks and security/encryption software loaded on the mobile devices and network infrastructure Enterprise applications integration includes back office applications, legacy systems, security, and all the other aspects of Central Bank of India.
- The Mobile Device Management module is essential solution required by Bank to manage, monitor and support use of mobile devices.
- The proposed Mobile Device Management solution should be able to address the following key areas but not restricted:
 1. Configuration of the solution balancing critical document access requirements with data security assurance
 2. Tying mobility to strategic business objectives
 3. Identifies key business processes that can be improved with mobilization
 4. Defines business process improvements
 5. Devise business and technical alignment with Bank's requirement
 6. To implement every aspect of the identified and designed mobility initiative, including architecture and systems integration
 7. Assists with device management and configuration
 8. Provides different devices application hosting options
 9. Provides help desk services
 10. Scalable, so new users and increasingly sophisticated devices can be accommodated easily
- The bidder must provide training to the identified Bank personnel/ SOC team on the product architecture, functionality and the solution design – to be provided before the implementation of solution.
- Provide hands-on training to the Bank personnel/ SOC team on MDM policy configuration, alert monitoring, problem mitigation and etc. post implementation.
- The bidder must integrate MDM with SIEM to generate alerts for any MDM violations.
- The Bidder needs to ensure the proposed solution is configured to generate events for monitoring through SIEM
- Bidder is responsible for migration of all the data and policies from existing solution to the proposed solution.
- Sizing Guidelines for Mobile Device Management can be found in Annexure 2 - Minimum Technical Specifications, in the subtab titles "Solutions Sizing".
- The Mobile Device Management solution should provide actionable reports, such as but not limited to below mentioned reports:
 1. Device Inventory and Management Reports - The MDM Solution should provide detailed list of all managed devices with their specifications, assessment of device compliance with security policies, analysis of operating system versions across devices, detailed information about device hardware and installed software.

2. Application Management Reports - The MDM Solution should provide list of installed applications on managed devices, assessment of application compliance with security policies and tracking of app deployment and updates.
3. Security and Compliance Reports - The MDM Solution should evaluate device security status, identify compromised (Jailbroken / rooted) devices, assess password strength.

7.1.10 Secure Data Backup and Recovery (Ransomware Protection)

- The bidder is required to Supply, Install, configure and Maintain “Database Recovery and Ransomware Protection (Ransomware Protection)” solutions at Bank for the period of contract. The proposed solution is required to meet the technical specifications and bill of material given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.
- Bidder is required to configure Database Recovery and Ransomware Protection at DC as Primary and at Disaster Recovery site as secondary, having high availability across DC and DRC. In case of DR Drill or DC fails, Database Recovery and Ransomware Protection at DRC should act as Primary.
- Bidders is required to provide must provide “Database Recovery and Ransomware Protection” solution to protect ransomware / Cyber Attack or data corruption for Bank's Oracle Databases having following features
 1. The proposed Database Recovery and Ransomware Protection solution should support real -time data protection ensuring near zero data loss
 2. The proposed solution must be sized for Oracle Database to cater to the workload with minimum 500 TB of usable capacity.
 3. For detailed functional and technical specifications, refer to Annexure 2 – Minimum Technical Specifications
- The proposed solution must be sized for Oracle Database and other databases’ Workload with minimum 500 TB usable capacity
- Sizing Guidelines for Secure Data Backup and Recovery can be found in Annexure 2 - Minimum Technical Specifications, in the subtab titles "Solutions Sizing".
- The Secure Data Backup and Recovery (Ransomware Protection) solution should provide actionable reports, such as but not limited to below mentioned reports:
 1. Should show the status of ongoing and completed backups, identify backup failures and their causes, measure the time taken to recover data
 2. Provide unified dashboard showing Database recoverability status and protection policy for all source databases, with the ability to drill down further.

7.1.11 Network Access Control (NAC)

- The bidder is required to Supply, Install and Maintain “Network Access Control” solutions at Bank for the period of contract. The proposed solution is required to meet the technical specifications and bill of material given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.
- Bidder is required to configure Network Access Control at DC as Primary and at Disaster Recovery site as secondary, having high availability across DC and DRC. In case of DR Drill or DC fails, Network Access Control at DRC should act as Primary
- The Bank intends to procure a Network Access Control solution that should enforces policies to ensure only authorized and compliant users and devices can access Bank’s network.

- The proposed NAC Solution should provide below mentioned key features to enhance Bank's network security:
 1. Endpoint Assessment: NAC should evaluate the security posture of devices attempting to connect to the network including wired and wireless network. It should include checking for antivirus software, firewall status, vulnerable application and operating system patches.
 2. Policy Enforcement: Based on the assessment results, NAC should enforce policies to allow, restrict, or deny access. Non-compliant devices may be quarantined or provided with limited access.
 3. Authentication and Authorization: NAC should verify the identity of users and devices before granting access. This should typically involve authentication methods like usernames/passwords, tokens, or biometrics.
 4. Guest Network Management: NAC should create and manage separate guest networks with restricted access, allowing for secure internet access for visitors or any other 3rd party user access.
 5. Compliance Enforcement: NAC should help Bank to comply with Government regulations by ensuring that only authorized devices and users with the necessary permissions can access sensitive data.
 6. Device Profiling: NAC should gather information about devices, such as manufacturer, model, and operating system, to identify potential security risks.
 7. Network Visibility: NAC should provide visibility into all devices connected to the network, making it easier to identify unauthorized or compromised systems.
 8. Threat Detection and Prevention: NAC should detect and prevent threats like malware, unauthorized access, and policy violations based on intelligence from the existing security solutions and block the assets automatically.
 9. Integration with Other Security Tools: NAC should integrate with other security solutions, such as firewalls, IPS, EDR and SIEMs, to provide a comprehensive security posture.
 10. Automation: NAC should automate many tasks, such as policy enforcement and device onboarding, to reduce administrative overhead.
- In case of failure of NAC appliance/ software, the Bidder shall provide redundant solution in no more time than 4 hours for any location wherever NAC is deployed.
- The Bidder is required to supply, implement & maintain NAC for:
 1. 36000 Endpoints (Includes DC, DRC, Branches. ATMs and Kiosks) and solution should be scalable to support 41000 endpoints during the period of contract.
 2. The solution is to be deployed at DC in HA mode and at DRC in HA mode.
 3. The NAC solution must Integrate with SIEM to generate alerts for any NAC violations.
 4. The responsibility of integration of solutions with existing SIEM lies with the Bidder selected through this RFP
 5. The Bidder needs to ensure the proposed solution is configured to generate events for monitoring through existing SIEM and EDR.
 6. The bidder/OEM must provide training to the identified Bank personnel/ SOC team on the product architecture, functionality and the solution design – to be provided before the implementation of solution.
 7. The bidder/OEM must provide hands-on training to the Bank personnel/ SOC team on NAC policy configuration, alert monitoring, and etc. post implementation.

- The Network Access Control (NAC) solution should provide actionable reports, such as but not limited to below mentioned reports:
 1. Device and User Activity Reports – The NAC solution should provide reports of user activity such as Logs of user logins, logouts, and network access attempts, including usernames, device information, and access times. The NAC solutions should also provide reports on the compliance status of devices based on predefined policies, including antivirus status, patch levels, and firewall configurations.
 2. Security Incident Reports – The NAC solution should provide reports on Security Alerts via notifications of potential security threats, such as malware detections, unauthorized access attempts, or policy violations.
 3. Compliance and Audit Reports – The NAC solution should provide Audit Trails with Logs of all administrative actions performed on the NAC system, including changes to policies, configurations, and user permissions.
 4. Custom Reports – The NAC solution must allow for custom reports including Data Export with export of report data in various formats (e.g., CSV, PDF) for further analysis or integration with other systems.

7.2 Detailed Scope of work for Facility Management Services

- As a part of FMS, the Bidder shall provide services relating to maintenance and support of Security Solutions and associated hardware.
- The Bidder shall consider and envisage all services that will be required in the maintenance and the management of the Security Solutions.
- The services must meet the service levels mentioned in the RFP document.
- Bidder is required to perform the following below mentioned activities, but not limited to:
- Coordination of warranty repair or replacement service for Hardware and process warranty claims, as applicable. If the equipment is required to be taken outside the Bank premises, the cost of transportation and other related costs will be borne by the Bidder.
- Coordinating and scheduling maintenance activities with the End User and appropriate support functions of the Bank (e.g. network support, facilities support, etc.)
- Provision of recovery procedures to maintenance personnel of the Bank
- Maintain accurate documentation on the current location and status of Hardware in the process of being repaired
- Services including requirement analysis, assisting the YIL in hardware and system software platform acquisition, testing, verification, and installation. The Bidder accepts that these services allow access to business-critical software and also agrees that services provided include implementation and maintenance of the hardware as well as installation of the licensed software.
- Hardware maintenance services including preventive Hardware support, preventive maintenance, corrective maintenance to remedy a problem, and scheduled maintenance required to maintain the Hardware in accordance with manufacturers' specifications and warranties
- Provide maintenance data.
- Provide a single-point-of-contact to End Users for the resolution of Hardware related problems or to request an equipment upgrade or consultation. If the Hardware supplied by the Bidder is to be replaced permanently, then the Bidder shall replace the equipment of same Make/Model/configuration or of higher configuration.
- Provide support and assistance, as required, to isolate complex network, operational and software problems related to the proposed solutions and infrastructure

- Track and report observed Mean Time Between Failures (MTBF) for Hardware and/or software.
- Backup, remove, protect, and restore programs, data and removable storage media in a machine prior to presenting the machine for service
- Bidder is required to provide the following resources at the Bank premises to provide support as per the below table –

S. no	Time Window	No. of Resources
1	8 AM – 8 PM	6 x L1 Resources 2 x L2 Resources
2	8 PM – 8 AM	2 x L1 Resources

- Out of the resources mentioned above, 1 x L1 Resource in the 8 AM – 8 PM shift should have adequate experience in carrying out Red Team Exercise and should be able to carry out Red Team Exercises as and when required by the Bank.
- Resources must have back lining support with the OEMs of the proposed solutions to provide 24x7x365 support for the Bank’s security solutions part of this RFP.
- L1 should have minimum 1 years of experience
- L2 should have minimum 4 years of experience
- Bank has the option to increase the number of L1 and L2 resources at the same rate quoted by the bidder for the duration of the contract.

8. General Responsibility of the Bidder

- For the Security solutions mentioned in the Bill of Material in Appendix 1, Bank has provided the minimum technical specification in Annexure 2.
- Bidders need to ensure that the solutions proposed are comply with these minimum technical requirements. The Bidder shall provide the sizing of the solution based on the information provided by the Bank in this RFP and Annexure 2 - of Minimum Technical Requirements. The Bidder shall provide the details of each individual solutions proposed along with the Hardware & software proposed, in Appendix 1 – Bill of Materials.
- Any components required for the successful implementation of the project should be the responsibility of the bidder.
- Bank is having EULA arrangement for Oracle. Accordingly, if the database proposed by the vendor is Oracle, no cost is to be mentioned. However, the license requirement should be clearly mentioned separately in the technical offer/document. If the proposed database is other than Oracle, the cost (original cost as well as ATS) should be mentioned and will be included in TCO.
- The Bidder shall provide the details of each individual solutions proposed along with the Hardware & software proposed in the RFP.
- Bidder should ensure dual power supply for all proposed solutions.
- Required racks, Network cables, and other component required for the successful implementation of the project should be the responsibility of the bidder. Bidder to provide the requirement at the time of bid submission.
- 42U Rack with dual PDU and perforated doors (600x800)
- All the equipment should be Rack Mountable and should have dual Power supply units.

- LTO8 Library based backup solution should be provided with backup software and necessary licenses. Feature online backup should be available.
- In case the bidder proposes any alternate solution in place of backup solution as mentioned above, they should be able to provide back up in removable device (tapes) to enable the bank for offsite storage of backup.
- The Bidder should take adequate care to avoid quoting security equipment that will become end of sale within 2 years of supply to the Bank and end of support within 7 years from the date of the submission of offer. In case any hardware / component reaches end of support during the contract period, bidder has to replace the same with new one, including successful installation and migration of data at no additional cost to the Bank. Failure to replace the product well in time by the actual end of support date will be treated as violation of SLA. Bank will procure new solution in such case and cost will be deducted from payables / payments as a penalty or by invoking PBG.
- The Bidder is required to procure, supply, install and provide subsequent comprehensive on-site warranty/AMC/ATS of the security equipment based on the Bill of Materials shared by the Bank and the solutions (Hardware, software, etc.) proposed and included in the Bill of Material by the Bidder for the security solutions.
- The delivery plan must be synchronized with the project delivery timelines of the Bank. Bidder is required to make available required resources that may be required for the successful completion of the entire assignment within the quoted cost to the Bank.

Delivery, Installation and Maintenance

- As a part of implementation of Cyber Security Solutions and associated hardware, the Bank expects the successful Bidder to provide power, space, and cooling requirements for the equipment to be hosted at DC and DRC. However, the hosting environment requirement shall be provided by the Bank at Bank's DC and DRC.
- Bidder should coordinate with the SPOC (DC/DR) for all the assignments relating to this RFP.
- Bidder is responsible for delivery, transportation, transit insurance – including insurance till installation acceptance by the Bank or its appointed consultant, unpack, racking and stacking, installation, and configuration of Cyber Security Solutions and associated hardware at DC, DRC and Central Office and other locations.
- The Bidder to do Power on self-test, basic configurations, migration, and installation of the equipment.
- Installation of the solutions is to be performed by OEM / OEM authorised partner for each solution.
- Any delay in installation of the Cyber Security Solutions and associated hardware for whatsoever reasons should not entail in expiry of insurance and the same should be continued and extended up to the date of installation and acceptance of the delivered Cyber Security Solutions and its associated licenses by the Bank.
- Bidder shall ensure compatibility of the supplied Cyber Security Solutions, hardware and licenses with the hardware and software systems being used in the Bank. In case of any compatibility issue arises between the proposed Cyber Security solution/appliance in existing setup during implementation or within 3 months of installation signoff, then the successful bidder is required to replace such solution/appliance, with the compatible one, at no additional cost to the bank within 4 weeks of the issue is identified by Bank or Bank's existing SI.

- Bidder should adhere to the service levels including delivery timelines specified in the RFP for the installation of Cyber Security Solutions and associated hardware supplied by them.
- In case of Hardware based Solutions, bidder shall provide replacement component from the same OEM, if any component is required to be taken out of the premises for repairs.
- Bidder must ensure that on call OEM support can be made available within one hour during the tenure of the contract.
- Bidder should ensure Knowledge Transfer to the Bank throughout delivery of the service, which should include detailed overview of the implementation and configuration parameters and features and functionality of the proposed Cyber Security Solutions.
- Bidder is required to provide acceptance of Purchase Order, within 7 days of issuance of PO to the Bank.
- All the components of this RFP should be covered under 24x7x365 direct OEM support for the tenure of the contract; that is the replacement of the defective components should be delivered within four hours from the time call is logged.

9. Project Timelines

The successful Bidder is expected to adhere to the following timelines concerning the implementation of the Cyber Security Solutions and associated hardware at Bank's DC and DRC:

#	Activity	Time for Delivery	Time for Installation	Time for Go Live
1	Delivery, Installation and Go Live of each of the individual solutions part of the RFP	10 Weeks from the acceptance of Purchase Order.	14 Weeks from the date of acceptance of purchase order.	24 Weeks from the date of acceptance of purchase order.

The Bank, at its discretion, shall have the right to alter the delivery schedule and quantities based on the implementation plan. This will be communicated formally to the Bidder during the implementation, if need arises.

Bank can also prioritize the implementation of the offered solutions part of the RFP and the priority of the same will be informed to the successful bidder during the implementation. In such case, project timelines will start from the date of intimation by the Bank.

10. Staggered delivery of the equipment's.

Bank may ask for staggered delivery of some of the Cyber Security Solutions and associated hardware mentioned in the RFP. Details of the same would be shared with the successful Bidder at a later stage.

11. Repeat Order (Right to Alter Quantities)

Bank may procure additional components up to 25% of the ordered quantity during the contract period at the same cost mentioned in Annexure 1: Bill of Material.

12. Contract Renewal

Bank, at its discretion, can opt to renew the contract for additional period of time on mutually agreed terms with the Bidder.

13. SLA compliance

Bidder should ensure compliance with SLAs as defined in the RFP.

13.1.1 Service Level Agreements (SLA)

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

13.1.2 Service Levels During Implementation Phase

- The Bidder is expected to complete the responsibilities that have been assigned as per the implementation timelines mentioned in Section 1.4 Project timelines.
- One percent of the total product cost for each solution would be levied as a penalty for every one-week delay as per implementation timelines per product/service.

Penalty would be levied for delayed delivery, installation, and implementation delays for each solution and shall be a maximum of 10% of the total cost of that solution from the finalized Bidder for the Bank. The Bidder is required to adhere to the Service Level Agreements as mentioned below for the operations phase.

The Bidder is required to adhere to the Service Level Agreements as mentioned below for the operations phase.

13.1.3 RMA (Return Merchandise Authorization):

For devices at DC/DR: Replacement for faulty equipment's must be done by bidder and follow up with OEM must be done by bidder only. RMA of Faulty equipment's should be received within 4 hours from the date of call lodge. In case bidder fails to provide the RMA of faulty/ damage equipment's penalty of 1% of equipment's cost weekly or part thereof maximum 10% of total contract value. However maximum cap of penalty will be 10% of total contract value.

13.1.4 Service Levels post acceptance of solutions by the Bank

Sr. No	Service Area	Service Level	Penalty
1	Individual Solutions Uptime	Uptime % calculated on monthly basis for each solution. In case of any hardware problems, the SI should ensure that replacement devices are made available to meet the SLAs.	Penalty (as mentioned Below) of the monthly FMS charges. These penalties will be deducted against any subsequent payable amount by the Bank like FMS / AMC / ATS etc.whichever is higher
		99.9% and above	NA
		98% to 99.89%	5%
		95% to 97.99%	8%
		90% to 94.99%	15%
		80% to 89.99%	30%
		70% to 79.99%	50%

Sr. No	Service Area	Service Level	Penalty
		Less than 70%	100%

13.1.5 Monitoring and Operations

Sr. No	Service Area	Expected Service Level	Penalty
1	Incident Response	<p>24x7 monitoring of all in-scope devices</p> <p>Categorization of events into Critical, High, Medium and Low priority shall be carried out in consultation with the selected Bidder during the contracting phase.</p>	<p>All Critical, High and Medium priority incident should be logged as incident tickets and responded as per below SLAs:</p> <p>Incident along with action plan/mitigation steps should be alerted to designated Bank personnel as per the below SLA:</p> <ul style="list-style-type: none"> • Critical incidents within 15 minutes of the incident identification. Update should be provided every 15 minutes till the closure of the incident. • High priority incidents within 30 minutes of the incident's identification. Update should be provided every 1 hour till the closure of the incident • Medium priority incidents within • 60 minutes of the incidents identification. Update should be provided every 4 hours till the closure of the incident. <p>Penalty: SLA is measured on a monthly basis and the penalty is as follows:</p> <p>Critical Events:</p> <ul style="list-style-type: none"> • 95-99%: 10% of the FMS cost for the Month • 90-95%: 15% of the FMS cost for the Month • <90%: 20% of the FMS cost for the Month

			<p>High Priority Events:</p> <ul style="list-style-type: none"> • 95-99%: 5% of the FMS cost for the Month • 90-95%: 10% of the FMS cost for the Month • <90%: 15% of the FMS cost for the Month <p>Medium Priority Events:</p> <ul style="list-style-type: none"> • 95-99%: 2% of the FMS cost for the Month • 90-95%: 5% of the FMS cost for the Month • <90%: 10% of the FMS cost for the Month <p>Low Priority/ Operational Incidents need to be logged and maintained for reference. An incident ticket need not be raised for such incidents. However, these need to be included in the daily reports.</p>
2	<p>Incident Response</p>	<p>Response and resolution of the identified incidents.</p> <p>Managing the devices and fine-tuning them so as to avoid and prevent further attacks.</p>	<p>The timelines required for resolution of Critical, High and Medium priority mentioned below:</p> <ul style="list-style-type: none"> • Disaster or Critical incidents within 60 minutes of the incident identification. Update should be provided every 15 minutes till the closure of the incident • High priority incidents within 90 minutes of the event identification. Update should be provided every 1 hour till the closure of the incident. • Medium priority incidents within 120 minutes of the event identification. Update should be provided

			<p>every 4 hours till the closure of the incident.</p> <p>Penalty:</p> <ul style="list-style-type: none"> Any violation in meeting the SLA requirements which leads to Critical incident, Bank shall impose a penalty 10% of the overall monthly operation charges for each 30 minutes delay up to 2 hours, beyond 2 hours penalty would be 10% of the overall monthly operation charges for each 20 minutes delay. Any violation in meeting the SLA requirements which leads to High or Medium incident, Bank shall impose a penalty of 5% of the overall monthly operation charges for each 45 minutes delay up to 3 hours, beyond 3 hours penalty would be 10% of the overall monthly charges for each 30 minutes delay.
3	Report and Dashboard	Periodic reports to be provided to Bank	<p>Daily Reports: Critical reports should be submitted as and when required. Timings will be mutually decided.</p> <p>Penalty Delay in reporting for daily report for more than 1 hour shall incur a penalty of 5% of FMS cost for the Month</p> <p>Weekly Reports: To be decided mutually</p> <p>Penalty Delay in reporting by more than 3 days for weekly reports shall incur a penalty of 3% of Operations</p>

			<p>Cost for the Month</p> <p>Monthly Reports: 5th of each month</p> <p>Penalty Delay in reporting by more than 3 days for monthly reports shall incur a penalty of 5% of FMS cost for the Month</p>
4	Continual Improvement	<ul style="list-style-type: none"> The Bidder is expected to improve the operations on an on-going basis. The Bidder is expected to provide a quarterly report of the new improvements suggested, action plans, and the status of these Improvements to the Bank. Improvement areas could include: process changes/ training resulting in efficiency/SLA improvement, new correlation rules to identify threat patterns etc. 	<p>Quarterly reports need to be provided by the 5th day of each quarter beginning</p> <p>Penalty: Delay in providing quarterly reports shall lead to 5% penalty of the monthly FMS charges Reduction by in the time for event response, quarter on quarter.</p>
5	Periodic Review	The project sponsor or locational delegate from the Bidder is expected to conduct a monthly review meeting with Bank officials resulting in a report covering details about current SLAs, status of operations, key threats and new threats identified, issues and challenges etc.	<p>Monthly review meeting to be conducted on the 5th (tentatively) of each month during the operations phase.</p> <p>Penalty: A delay of more than three days will incur a penalty of 5% of FMS cost for that month.</p>
6	Security Device and Management	Bidder is expected to provide this service 24/7	<p>Penalty:</p> <ul style="list-style-type: none"> For more than 1 hour

	Administration	basis. Management and administration of all existing and in-scope security devices / solutions	<p>delay (after the Banks confirmation) for rule modification in any of the security devices / solutions will incur a penalty of 2% of monthly FMS cost per instance.</p> <ul style="list-style-type: none"> For wrong rule modification in any of the security solutions will incur a penalty of 5% of the monthly FMS cost per instance. For a wrong rule modification in any of the security solutions by which Bank incur any service disturbance will incur a penalty of 10% of monthly FMS cost per instance.
7	IT Governance Risk and Compliance	The Bidder is expected to provide reports dashboards on ad-hoc basis as and when required by Bank. Bidder must provide a written/email based response to the requested dashboard/report mentioning the time of delivery of report/dashboard Service uptime SLA shall apply after the time of delivery as declared by the Bidder.	Penalty: Bidder failing to respond back with details of dashboard/report availability shall be penalty of 5% of the monthly FMS charges.
8	Proactive monitoring against any security incident/breach	Bidder is expected to proactively monitor Bank's network to defend against any cyber incident/breach	Penalty: If any security breach happens in Bank's network during contract period because any of below given reasons, Penalties will be levied @ ₹ 1,00,000/- per instance or equal to the loss of amount, if any (whichever is higher): <ul style="list-style-type: none"> Lack of proactive monitoring Improper configuration of in- scope devices

			<ul style="list-style-type: none"> • Violation in defined policies • Alert not handled/closed properly • Any fraud/data theft/misconduct committed by Bidder's resource causing business/reputation/operation loss to Bank. <p>The penalty will be restricted to the yearly payout value.</p>
--	--	--	---

- Note : During the contract period, if any other requirement not mentioned above but part of the contract if not fulfilled by bidder / OEM within the timeline will be considered as non-compliance and liable for penalty of flat 0.5% of the TCO of that solution.

13.1.6 Responsibility Matrix

The following table describes the responsibilities of the Bidder, Bank and original equipment manufacturer for problem management and issue resolution related to the applications and tools hosted on the hardware and software proposed by the Bidder.

Sr. No	Activity	Bank	Bidder	OEM
1	Solution Designing	S	P	V & M
2	Installation of the proposed hardware and software including configuration as per the solution design	S	P	V & M
3	Acceptance of the solution	S	P	-
4	SLA Reports	S	P	-
5	Incident Management	S	P	P
	<p>S – Signed Off (Responsible for providing the go-ahead) P – Performed (Primary responsibility for executing the activity) V – Validated (Responsible for Validating the activity) M – Monitoring (Responsible for continuous monitoring of activity)</p>			

13.1.7 Penalty Computation

In the event of Service Level Default, Bidder shall pay the Bank a penalty that will be computed in accordance with the following formula:

Monthly Service Level Default = Minimum Service Level (for a month) – Actual Service Level (for a month)

Total amount of penalty Bidder is obligated to pay the Bank shall be reflected on the invoice provided to the Bank in the quarter, after the quarter in which the Service Levels were assessed. The Bank shall be entitled to deduct the penalty amount from the amounts payable by the Bank to the selected Bidder as per the invoice.

Example:

Scenario	Result
The achieved availability of Network Infrastructure has been measured to be 98% in a particular assessment month.	<p>The expected Availability service level for Cyber Security Solutions and associated hardware is 99.95%.</p> <p>The achieved service level in the assessment month was calculated to be 98%</p> <p><u>Cost Reference for 5 year tenure</u></p> <p>Cyber Security Solutions cost = INR 1 crores (approximately)</p> <p>Cyber Security Solutions AMC cost (till date) = INR 30,00,000 (approximately)</p> <p>Total cost of product and services for a Cyber security Solutions = 1,30,00,000</p> <p>As per above table, for Availability Service level default of more than 99.5% and less than 98%, a penalty of 2% would be levied of the total cost of products and services calculated above.</p> <p>Thus, 2% of 1,30,00,000 i.e. INR 2,60,000.</p>

14. Liquidated damage

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

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

The Liquidated Damages (LD) shall be 1 % of TCO amount (excluding FMS) for the respective solution, which have been delayed for each week or part thereof for delay until actual delivery or performance. However, the total amount of Liquidated Damages deducted will be pegged at 10% of the contract value. Once the maximum is reached, the Bank may consider termination of the contract and other penal measure will be taken like forfeiture of EMD, Foreclosure of BG etc.

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

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

15. Land Border Sharing Clause

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

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

- i. Any bidder from a country which shares a land border with India will be eligible to bid in this tender only if the bidder is registered with Competent Authority.
- ii. "Bidder" (including the term 'tenderer', 'consultant' or 'service provider' in certain contexts) means any person or firm or company, including any member of a consortium or joint venture (that is an association of several persons, or firms or companies), every artificial juridical person not falling in any of the descriptions of bidders stated hereinbefore, including any agency branch or office controlled by such persons, participating in a procurement process.
- iii. "Bidder from a country which shares a land border with India" for the purpose of this Order means:
 - a. An entity incorporated, established, or registered in such a country; or
 - b. A subsidiary of an entity incorporated, established or registered in such a country; or
 - c. An entity substantially controlled through entities incorporated, established or registered in such a country; or
 - d. An entity whose beneficial owner is situated in such a country; or
 - e. An Indian (or other) agent of such an entity; or
 - f. A natural person who is a citizen of such a country; or
 - g. A consortium or joint venture where any member of the consortium or joint venture falls under any of the above.

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

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

Explanation

- a. "Controlling ownership interests" means ownership of or entitlement to more than twenty five per-cent of shares or capital or profits of the company.
- b. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholder's agreements or voting agreements.
2. In case of partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together or through one or more judicial person, has ownership of entitlement to more than fifteen per-cent of capital or profits of the partnership.
3. In case of an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together or through one or more judicial person, has

ownership of or entitlement to more than fifteen per-cent of the property or capital or profits of such association or body of individuals.

4. Where no natural person is identified under (1) or (2) or (3) above, the beneficial owner is the relevant natural person(s), who hold the position of senior managing official.
5. In case of trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen per-cent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.
 - iv. An agent is a person employed to do any act for another, or to represent another in dealings with third persons.

16. Monitoring & Audit

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

17. Bid Submission

- All responses received after the due date/time be considered late and would be liable to be rejected. E-procurement portal will not allow lodgement of RFP response after the deadline. It should be clearly noted that the Bank has no obligation to accept or act on any reason for a late submitted response to RFP. The Bank has no liability to any Respondent who lodges a late RFP response for any reason whatsoever, including RFP responses taken to be late only because of another condition while responding.
- "Cost of Tender Document" may be paid through RTGS (Real Time Gross Settlement) / NEFT favouring CENTRAL BANK OF INDIA, BANK ACCOUNT NO.-3287810289, IFSC CODE - CBIN0283154 or by way of Bankers Cheque/Demand Draft/Pay Order favouring Central Bank of India, payable at Mumbai, which is non-refundable, must be submitted separately along with RFP response. The RFP response without proof of payment of application money or cost of tender document shall not be considered and shall be rejected, except in case of bidder being MSME as per the exemption applicable to it.
- The details of the transaction viz. scanned copy of the receipt of making transaction are required to be uploaded on e-procurement website at the time of "final online bid submission The RFP response without proof of amount paid towards Application Money / Bid Security are liable to be rejected.

Instructions to Bidders: e-tendering

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

Preparation & Submission of Bids

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

Do's and Do not's for Bidder

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

Terms & Conditions of Online Submission

1. Bank has decided to determine L1 through bids submitted on GeM portal. Bidders shall bear the cost of registration on the GeM portal. Bidder is bound to follow rules of GeM portal as per Government guidelines.
2. Bidders at their own responsibility are advised to conduct a mock drill if required.
3. In the event of failure of the internet connectivity (due to any reason whatsoever it may be) Bank will not be responsible.
4. In order to ward-off such contingent situation, Bidders are advised to make all the necessary arrangements / alternatives such as back –up power supply, connectivity whatever required so that they are able to circumvent such situation and still be able to participate in the Auction successfully.
5. However, the bidders are requested to not to wait till the last moment to quote their bids to avoid any such complex situations.
6. Failure of power at the premises of bidders during the E-Tendering cannot be the cause for not participating in the E-Tendering.
7. On account of this, the time for the E-Tendering cannot be extended and BANK is not responsible for such eventualities.
8. Bank will not have any liability to Bidders for any interruption or delay in access to site of E-Tendering irrespective of the cause.

Tender Schedule (Key Dates)

The Bidders are strictly advised to follow the Dates and Times as indicated in the Time Schedule in the detailed tender Notice for the Tender. All the online activities are time tracked and the electronic Tendering System enforces time-locks that ensure that no activity or transaction can take place outside the Start and End Dates and time of the stage as defined in the Tender Schedule.

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

18. Integrity Pact

Each Participating bidder/s shall submit Integrity Pact as per attached Annexure 9 duly stamped for ₹500. Integrity pact should be submitted by all participating bidders at the time of submission of bid documents or as per satisfaction of the Bank. The Non submission of Integrity Pact as per time schedule prescribed by Bank may be relevant ground of disqualification for participating in Bid process.

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

Sri Anant Kumar [mail: mailto:anant_in@yahoo.com]

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

19. Commercial Offers

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

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

- a. The commercial offer should be in compliance with technical configuration / specifications as per Technical Specifications.
- b. The price to be quoted for all individual items and it should be unit price in Indian rupees.
- c. In case there is a variation between numbers and words, the value mentioned in words would be considered. The Bidder is expected to quote unit price in Indian Rupees (without decimal places) for all components and services on a fixed price basis, as per the commercial Bid inclusive of all costs. GST (Goods and Services Taxes) shall be payable as per applicable structure laid down under GST Law. The Bank will not pay any other taxes, cost, or charges. The price would be inclusive of all applicable taxes under the Indian law like customs duty, freight, forwarding, insurance, delivery, etc. but exclusive of only applicable GST, which shall be paid/ reimbursed on actual basis on production of bills with GSTIN. Any increase in GST will be paid in actuals by the Bank or any

new tax introduced by the government will also be paid by the Bank. The entire benefits/ advantages, arising out of fall in prices, taxes, duties or any other reason, must be passed on to Bank. The price quoted by the Bidder should not change due to exchange rate fluctuations, inflation, market conditions, and increase in custom duty. The Bank will not pay any out-of-pocket expense. The Selected Bidder will be entirely responsible for license fee, road permits, insurance etc. in connection with the delivery of products at site advised by the Bank including incidental services and commissioning.

- d. The price is exclusive of taxes i.e. Goods and Services Tax, which shall be paid as per actuals.
- e. Bank will award the contract to the successful Bidder, whose bid has been determined as the Lowest Commercial bid (L1) through the Reverse Auction process of this commercial evaluation through GeM Portal.

20. Evaluation & Acceptance

1. Technical offers will be evaluated on the basis of compliance with eligibility criteria, technical specification, other terms & conditions stipulated in the RFP. Only those bidders who qualify in the technical evaluation would be considered for evaluating the commercial bid. Bank may, at its sole discretion, waive any non-conformity or deviations.
2. Bank reserves the right to reject the bid offer under any of the following circumstances: a) If the bid offer is incomplete and / or not accompanied by all stipulated documents. b) If the bid offer is not in conformity with the terms and conditions stipulated in the RFP. c) If there is a deviation in respect to the technical specifications of hardware items.
3. The Bank shall be under no obligation to mandatorily accept the lowest or any other offer received and shall be entitled to reject any or all offers without assigning reasons

21. Evaluation Process

The competitive bids shall be evaluated in three phases:

- Stage 1 – Eligibility Criteria Evaluation Stage - Bidder have to qualify each and every criteria as mentioned in the section 2 of the RFP, to qualify for the next stage of evaluation.
- Stage 2 – Technical Evaluation Stage - Bidders Qualify in Stage 1 have to score minimum 70% marks in technical evaluation as per section 20.2 of the RFP to qualify for stage 3
- Stage 3 – Commercial Bid process / Reverse Auction
-

21.1 Eligibility Criteria Evaluation

Central Bank of India is looking for Supply, Installation and Maintenance of Cybersecurity Solutions and associated hardware at the Bank. It includes supply, installation, Implementation and maintenance of the Solution(s).

Only those Bidders who fulfil the following criteria are eligible to respond to the RFP. Offers received from Bidders who do not fulfil any of the following eligibility criteria will be summarily rejected.

Bidder will be responsible for delivering the end-to-end solution and will be the single point of contact for the implementation, integration, support and maintenance for the entire project. Bidder will also be solely responsible for ensuring adherence to the Service Levels, terms & condition and Service

Quality for each of the deliverables executed. However, OEM or its authorized service partners will be responsible for implementation.

The bidder must fulfil the criteria mentioned in the Section2 of this RFP:

Note:

- 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. Central Bank of India reserves the right to verify /evaluate the claims made by the Bidder independently. Any decision of Central Bank of India in this regard shall be final, conclusive, and binding upon the Bidder.
- 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.
- In-case of corporate restructuring the earlier entity's incorporation certificate, financial statements, Credentials, etc. may be considered.

21.2 Technical Evaluation Criteria

The bidder must fulfil the criteria mentioned in the Section2 of this RFP:

Note:

- 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. Central Bank of India reserves the right to verify /evaluate the claims made by the Bidder independently. Any decision of Central Bank of India in this regard shall be final, conclusive, and binding upon the Bidder.
- 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.
- In-case of corporate restructuring the earlier entity's incorporation certificate, financial statements, Credentials, etc. may be considered.

Detailed Evaluation Criteria

S. No	Criteria	Min Score	Max Score
1.	The bidding entity should have minimum annual average turnover of ₹ 500 Crores (Rupees Five Hundred crores) in last three financial years with audited reports (i.e. 2021-22, 2022-23, 2023-24) Turnover 500-750 Cr - 5 Marks Turnover 751-1000 Cr - 7 Marks Turnover above 1000 Cr - 10 Marks	5	10
2.	100% Compliance to Technical Specifications	30	30

3.	100% Compliance to Scope of Work	10	10
4.	<p>Bidder Implementation Experience - Number of Successful deployments by the Bidder for solutions offered in Scheduled Commercial Banks / BFSI having minimum 500 branches / offices in India:</p> <p>The bidder should have the experience of executing Purchase Orders/ Work Orders/ Contracts/ Reference</p> <p>4 – 5 Number of Solution – 10 Marks</p> <p>6 – 7 Number of Solution – 15 Marks</p> <p>More than 7 Number of Solution – 20 Marks</p>	10	20
5.	<p>Presentation by bidders on the following but not limited to -</p> <ul style="list-style-type: none"> • Approach and Methodology for Implementation • Solution Design • Resource Deployment Plan • Support Strategy 	10	20
6.	<p>The bidder must have minimum of 10 certified resources having certifications such as CISSP, CISA, CISM, CEH.</p> <p>10 – 20 certified resources - 5 marks</p> <p>21 – 30 certified resources - 7 marks</p> <p>More than 30 certified resources - 10 marks</p>	5	10
	TOTAL	70	100

The Minimum Qualifying Marks for Next Stage of evaluation is 70% i.e. 70 out of 100.

The Bank at its sole discretion may relax the cut-off score to a lower value, if required.

Note:

1. Bank may call for presentation(s), product walkthroughs, on the features of the solution offered etc., from the bidders based on the technical bids submitted by them.
2. Based upon the compliance of the minimum technical specifications of the proposed product / solution, shortlisting would be made of the eligible bidders for final commercial bidding.
3. Bank reserves the right to conduct reference site visits at the Bidder's client sites for verification of the compliance submitted by the bidder.
4. Bank reserves the right to conduct Proof of Concept for the offered solution without any additional cost to the Bank.
5. Bank reserves the right to disqualify the bidder / solution based on any of the above.

21.3 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 Reverse Auction process. The Bank will notify the date and time for participating in the online reverse auction process to the technically qualified bidders.

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

Bank will notify the name of the technically eligible bidders for participating in Reverse Auction.

At the end of reverse auction process, Bidder (L1) quoting the lowest bid will be selected on the basis of Total Price.

Reverse Auction

The Bank shall conduct the reverse auction on total cost of project and the price so obtained after closure of Reverse Auction shall be taken into account for Commercial Evaluation.

The L1 bidder should submit the detailed break up as per the BOQ format within 48 hours of closure of the reverse auction. The price breakup should contain not only the rates but also the value of each item of works/goods entered in a separate column and all the items as per the Bank. BOQ format totalled up in order to show the L1 aggregate value of the amount. Please note that bidder have to quote for the individual items mentioned in the tender as well as proposed by the bidder in there technical BOQ. L1 vendor, immediately on completion of the reverse auction activity, has to provide the unit-wise prices of all the items in the tender.

In case any technically qualified bidder does not take part in reverse action, then he will not be considered for commercial evaluation.

The procedure of reverse auction will be notified to the shortlisted bidders (Technically Qualified bidders) separately.

As per the GeM portal rules, the technically qualified Highest Quoting bidder will not be allowed to participate in Reverse Auction. However, H-1 will also be allowed to participate in RA in following cases:

- a. If number of technically qualified bidders are only 2 or 3.
- b. If Buyer has chosen to split the bid amongst N sellers, and H1 bid is coming within N sellers.
- c. In case Primary product of only one OEM is left in contention for participation in RA on elimination of H-1.
- d. If L-1 is non-MSE and H-1 is eligible MSE and H-1 price is coming within price band of 15% of Non-MSE L-1 as per applicability
- e. If L-1 is non-MII and H-1 is eligible MII and H-1 price is coming within price band of 20% of Non-MII L-1 as per applicability.

Date/time of reverse auction

1. The date and time of commencement of reverse auction also duration of 'Reverse Auction Time' shall be communicated to technically qualified bidders.
2. Any force majeure or other condition leading to postponement of auction shall entitle the Bank to postponement of auction even after communication, but Bank shall be obliged to communicate to all participating bidders the 'postponement' prior to commencement of such 'Reverse Auction'.

Conduct of Reverse Auction

The reverse auction shall be conducted as deemed fit by the Bank meant for this purpose.

Business Rules

Business Rules as may become emergent and based on the experience gained may be made by the Bank. Business rules shall be provided to the technically qualified bidders.

22. Payment Terms

The term of the contract will be 5 years. Hardware to be provided for execution of project should be sized for 5 years by considering functional & technical requirements as per in-scope solutions. However, if it is found that the hardware is not sized adequately or the hardware utilization goes beyond the threshold limit of 70%, the Bidder has to provide additional hardware at no additional cost to meet the performance parameters set by the Bank. The Bidder must accept the payment terms proposed by the Bank as proposed in this Section. The financial offer submitted by the Bidder after the reverse auction process must be in conformity with the payment terms proposed by the Bank. Any deviation from the proposed payment terms would not be accepted.

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

Payment for the Supply of required HW, SW, Design, Installation, Implementation, and Commission of the solutions shall be made by Bank as per the solutions in scope as mentioned in the Scope of Work.

22.1 Procedure for Claiming Payments

The Bidder's requests for payment shall be made to the Bank in writing accompanied by Original Invoice detailing the systems, software delivered, installed and accepted by the Bank. The payment after deducting applicable TDS will be released by the Bank. All payments will be made only by electronic transfer of funds either by NEFT or RTGS. The Bidder therefore has to furnish the Bank account number to where the funds have to be transferred for effecting payments. Payments as per the schedule given below will be released only on acceptance of the order and on signing the agreement / contract by the selected Bidder and also on submission of performance guarantee through a DD or Bank Guarantee in lieu of DD towards EMD.

The Bidder will have to submit a document explaining the AMC / ATS costs. The scope of work is divided in different areas, the payment would be linked to delivery, and acceptance of each area as explained below:

S. No	Deliverables	% Of Payment	Payment Milestone (On completion of the activities)
1	For Hardware of each Security Solutions at the Bank	70%	On post-delivery inspection of the product
		20%	Against successful installation and acceptance testing of the product signoff at DC, DRC
		10%	3 months after successful installation signoff
2	For Software of each Security Solutions at the Bank	60%	On post-delivery inspection of the product
		30%	Against successful installation and acceptance testing of the product signoff at DC, DRC
		10%	3 months after successful installation signoff
3	For FM Support	-	Payment for on-site support charges will be paid quarterly in arrears.

22.2 AMC/ATS Payment Terms

- AMC/ATS amount payable would be paid quarterly in arrears at the end of each quarter.
- First quarter for AMC/ATS payment would begin from 1st of the next month of the date of completion of the warranty period.
- In case bidder fails to have agreement with respective OEM's for back-to-back support after 3 years for hardware post warranty and for 1 year for software post warranty, the bank reserves the right to not make any payment for the duration for which Bidder was unable to produce the back-to-back agreement with the respective OEM to the Bank.

23. AMC & ATS and Warranty Costs

Bidder shall provide the maintenance (Warranty, AMC & ATS) for a period of five years from the date of successful installation of the product in CBol. Warranty period for the new components should be for the first three years for which the cost should be factored in the Product cost and AMC/ATS shall be factored for the subsequent two years. Bidder must factor the costs in the Bill of Material accordingly. As part of warranty, AMC & ATS support the Bidder must:

- Provide on-site comprehensive support for Cyber Security Solutions and associated hardware provided as part of this RFP
- Have back-to-back arrangements with respective OEMs for the maintenance services (Warranty/AMC/ATS)

- Warrant all the Cyber Security Solutions and associated hardware against defects arising out of faulty design, materials, and media workmanship etc., for a period of five years from the date of acceptance of the Cyber Security Solutions
- Provide maintenance of Cyber Security Solutions hardware as well as repair or replacement activity after hardware problem has occurred. If the supplied equipment are to be replaced permanently due to the Bidder's inability to provide spares or maintain the equipment, the Bidder shall replace the equipment of same make/ model/configuration or of higher configuration at no extra cost to the Bank. However, the Bank may accept different make/model/ configuration at its discretion, if the original make/model/ configurations are not available in the market due to obsolescence or technological up gradation
- Provide support services like repair, replacement to resolve the problem as per the service levels defined in this RFP.
- Defective Cyber Security Solutions hardware shall be replaced by the Bidder at his own cost, including the cost of transport etc. The Bidder shall not charge the Bank any extra charges related to this activity during the period of contract.
- Bidder may provide adequate spares for the critical components of the Cyber Security Solutions and associated hardware to meet the SLA.
- Provide expert person for onsite support during DR Drills / cyber drills / attack simulation exercises / audit etc as required by the Bank.
- The Bank will not be liable to pay any additional amounts in respect of any sort of maintenance covered under the scope of this tender during the tenure of the contract. Free on-site maintenance services shall be provided by Bidder during the period of warranty
- Bidder should undertake system maintenance and replacement or repair of defective Cyber Security Solutions hardware.
- In case equipment taken away for repairs, Bidder shall provide similar standby equipment so that the equipment can be put to use in the absence of the originals/ replacements without disrupting the Bank's regular work
- If during operation, the down time of any piece of equipment or component thereof does not prove to be within reasonable period, Bidder shall replace the unit of component with another of the same performance and quality or higher, at no cost to the Bank
- Further provided that the Bank may, during the contract, shift the goods wholly or in part to other location(s) within the Country and in such case the Bidder undertakes to continue to warrant or maintain the goods at the new location without any other additional cost to the Bank
- In case the Bank desires to get the services delivered by their appointed Bidder or System Integrator, then the OEM shall transfer such services to that preferred Bidder at no additional cost to the Bank.
- In case of any issue with Cyber Security Solutions and associated hardware supplied by Bidder, Bank shall log a call with Bidder (who has supplied the Cyber Security Solutions) it is responsibility of Bidder to resolve the issue with the assistance of the OEM if deemed necessary. The Bank or its appointed System Integrator shall promptly notify Bidder in writing/e-mail of any claims arising under the maintenance services.
- Provide all future software upgrades and patches for all components of the solution and assist the Bank or its System Integrator to install the same if Bank desires during period of contract at free of cost.

- Bidder warrants that the Goods supplied under the Contract are new & unused, of the most recent or current models and incorporate all recent improvements in design and materials unless provided otherwise in the RFP
- Bidder further warrants that all the Goods supplied under as part of this RFP shall have no defect arising from design, materials, or workmanship (except when the design and/or material is required by the Bank's Specifications) or from any act or omission of Bidder, that may develop under normal use of the supplied Goods in the conditions prevailing at the final destination
- Bidder's hardware engineer will report at the Bank's premises within one hour of reporting of breakdown and repair the same at the earliest.

The payments will be released through NEFT / RTGS/account credit after deducting the applicable LD/Penalty, TDS if any, on submission of invoices to DIT CBD- Belapur. The Successful Bidder has to provide necessary Bank Details like Account No., Bank's Name with Branch, IFSC Code, GSTIN, State Code, State Name, HSN Code etc.

Fixed Price

The commercial offer shall be on a fixed price basis, exclusive of all taxes and levies. No price variation relating to increases in customs duty, excise tax, dollar price variation etc. will be permitted. The bidder shall pay any other applicable Taxes being applicable after placement of order, during currency of the project only.

Taxes

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

- iv. If bidder as the case may be, is backlisted in the GST (Goods and Services Tax) portal or rating of a supplier falls below a mandatory level, as decided time to time may be relevant ground of cancellation of Contract.
4. Bank shall deduct tax at source, if any, as per the applicable law of the land time being enforced. The Service provider shall pay any other taxes separately or along with GST if any attributed by the Government Authorities including Municipal and Local bodies or any other authority authorized in this regard.

24. Order Cancellation

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

1. Delay in delivery beyond the specified period for delivery.
2. Serious discrepancy in hardware noticed during Installation or during maintenance period
3. Any other lapse pertaining to the order.
4. Penalty beyond 10% of the Total Project cost. In addition to the cancellation of purchase order, Bank reserves the right to appropriate the damages by foreclosing the performance bank guarantee.

25. Indemnity

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

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

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

- (i) The Bank notifies the Bidder in writing immediately on aware of such claim,
- (ii) The Bidder has sole control of defense and all related settlement negotiations,
- (iii) The Bank provides the Bidder with the assistance, information and authority reasonably necessary to perform the above, and
- (iv) The Bank does not make any statement or comments or representations about the claim without prior written consent of the Bidder, except under due process of law or order of the court. It is clarified that the Bidder shall in no event enter into a settlement, compromise or make any statement (including failure to take appropriate steps) that may be detrimental to the Bank's (and/or its customers, users and Bidders) rights, interest and reputation.

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

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

- i. that the Deliverables and Services delivered or provided under this Agreement infringe a patent, utility model, industrial design, copyright, trade secret, mask work or trademark in any country where the Deliverables and Services are used, sold or received; and/or The Bidder shall indemnify the Bank in case of any mismatch of ITC (Input Tax Credit) in the GSTR 2A, where the Bank does not opt for retention of GST component on supplies.
- ii. all claims, losses, costs, damages, expenses, action, suits and other proceedings resulting from infringement of any patent, trade-marks, copyrights etc. or such other statutory infringements under any laws including the Copyright Act, 1957 or Information Technology Act, 2000 or any Law, rules, regulation, bylaws, notification time being enforced in respect of all the Hardware, Software and network equipment or other systems supplied by them to the Bank from whatsoever source, provided the Bank notifies the Bidder in writing as soon as practicable when the Bank becomes aware of the claim however:
 - a. The Bidder has sole control of the defense and all related settlement negotiations.
 - b. The Bank provides the Bidder with the assistance, information and authority reasonably necessary to perform the above and bidder is aware of the rights to make any statements or comments or representations about the claim by Bank or any regulatory authority. Indemnity would be limited to court or arbitration awarded damages and shall exclude indirect and incidental damages and compensations.

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

- (i) Bidder's compliance with Bank's specific technical designs or instructions (except where Bidder knew or should have known that such compliance was likely to result in an Infringement Claim and Bidder did not inform Bank of the same);
- (ii) Inclusion in a Deliverable of any content or other materials provided by Bank and the infringement relates to or arises from such Bank materials or provided material;
- (iii) Modification of a Deliverable after delivery by Bidder to Bank if such modification was not made by or on behalf of the Bidder;
- (iv) operation or use of some or all of the Deliverable in combination with products, information, specification, instructions, data, materials not provided by Bidder; or (v) use of the Deliverables for any purposes for which the same have not been designed or developed or other than in accordance with any applicable specifications or documentation provided under the applicable Statement of Work by the Bidder; or
- (v) Use of a superseded release of some or all of the Deliverables or Bank's failure to use any modification of the Deliverable furnished under this Agreement including, but not limited to, corrections, fixes, or enhancements made available by the Bidder.

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

- (i) Procure for Bank the right to continue using such Deliverable;
- (ii) Modify the Deliverable so that it becomes non-infringing without materially altering its capacity or performance;
- (iii) replace the Deliverable with work product that is equal in capacity and performance but is non-infringing; or (iv) If such measures do not achieve the desired result and if the infringement is established by a final decision of the courts or a judicial or extrajudicial settlement, the Bidder shall refund the Bank the fees effectively paid for that Deliverable by the Bank subject to depreciation for the period of Use, on a straight line depreciation over a 5 year period basis. The foregoing provides for the entire liability of the Bidder and the exclusive remedy of the Bank in matters related to infringement of third party intellectual property rights.

The Bank warrants that all software, information, data, materials and other assistance provided by it under this Agreement shall not infringe any intellectual property rights of third parties, and agrees that it shall at all times indemnify and hold Bidder harmless from any loss, claim, damages, costs, expenses, including Attorney's fees, which may be incurred as a result of any action or claim that may be made or initiated against it by any third parties alleging infringement of their rights.

26. Confidentiality & Non-Disclosure

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

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

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

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

The bidder should undertake to maintain confidentiality of the Banks information even after the termination / expiry of the contracts.

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

Guarantee on Software License

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

27. Force Majeure

The parties shall not be liable for default or non-performance of the obligations under the contract, if such default or non-performance of the obligations under this contract is caused by any reason or circumstances or occurrences beyond the control of the parties, as a result of force majeure. For the purpose of this clause, "Force Majeure" shall mean an event beyond the control of the parties, including but not limited to, due to or as a result of or caused by acts of God, wars, epidemic/pandemic, insurrections, riots, earth quake and fire, events not foreseeable but does not include any fault or negligence or carelessness on the part of the parties, resulting in such a situation.

In the event of any such intervening Force Majeure, each party shall notify the other party in writing of such circumstances and the cause thereof immediately within seven business days. Unless otherwise directed by the other party, the party pleading Force Majeure shall continue to perform/render/discharge other obligations as far as they can reasonably be attended/fulfilled and shall seek all reasonable alternative means for performance affected by the Event of Force Majeure.

In such a case, the time for performance shall be extended by a period(s) not less than the duration of such delay. If the duration of delay continues beyond a period of three months due to force majeure situation, the parties shall hold consultations with each other in an endeavour to find a solution to the

problem. However bidder shall be entitled to receive payments for all services actually rendered upto the date of termination of date of agreement. The financial constraints by way of increased cost to perform the obligations shall not be treated as a force majeure situation if the obligations can otherwise be performed.

28. Resolution of Disputes

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

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

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

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

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

29. Independent Contractor

Nothing herein contained will be construed to imply a joint venture, partnership, principal agent relationship or co-employment or joint employment between the Bank and Bidder. Bidder, in furnishing services to the Bank hereunder, is acting only as an independent contractor. Bidder does not undertake by this Agreement or otherwise to perform any obligation of the Bank, whether regulatory or contractual, or to assume any responsibility for the Bank's business or operations. The parties agree that, to the fullest extent permitted by applicable law; Bidder has not, and is not, assuming any duty or obligation that the Bank may owe to its customers or any other person. The bidder shall follow all the rules, regulations statutes and local laws and shall not commit breach of any

such applicable laws, regulations etc. In respect of sub-contracts, as applicable – If required by the Bidders, should provide complete details of any subcontractor/s used for the purpose of this engagement. It is clarified that notwithstanding the use of sub-contractors by the Bidder, the Bidder shall be solely responsible for performance of all obligations under the SLA/NDA (Non-Disclosure Agreement) irrespective of the failure or inability of the subcontractor chosen by the Bidder to perform its obligations. The Bidder shall also have the responsibility for payment of all dues and contributions, as applicable, towards statutory benefits including labour laws for its employees and sub-contractors or as the case may be. Bidder should take bank's prior written permission before subcontracting/ resource outsourcing of any work related to the performance of this RFP or as the case may be, which permission shall not be unreasonably withheld by the Bank. The bidder should ensure that the due diligence and verification of antecedents of employees/personnel deployed by him for this project are completed and is available for scrutiny by the Bank.

30. Assignment

Bank may assign the Project and the solution and services provided therein by Bidder in whole or as part of a corporate reorganization, consolidation, merger, or sale of substantially all of its assets. The Bank shall have the right to assign such portion of the facilities management services to any of the Contractor/sub-contractor, at its sole option, upon the occurrence of the following: (i) Bidder refuses to perform; (ii) Bidder is unable to perform; (iii) termination of the contract with Bidder for any reason whatsoever; (iv) expiry of the contract. Such right shall be without prejudice to the rights and remedies, which the Bank may have against Bidder. Bidder shall ensure that the said sub-contractors shall agree to provide such services to the Bank at no less favourable terms than that provided by Bidder and shall include appropriate wordings to this effect in the agreement entered into by Bidder with such sub-contractors. The assignment envisaged in this scenario is only in certain extreme events such as refusal or inability of Bidder to perform or termination/expiry of the contract/project.

31. Execution of Contract, SLA & NDA

The bidder and Bank should execute

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

32. Vendor's Liability

The Bidder's (after entering into contract, to be called as the Vendor) aggregate liability in connection with obligations undertaken as a part of the project regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), shall be at actuals and limited to the value of the contract. The Bidders liability in case of claims against the Bank resulting from misconduct or gross negligence of the Bidder, its employees and subcontractors or from infringement of patents, trademarks, copyrights(if any) or breach of confidentiality obligations shall be unlimited. In no event shall the Bank be liable for any indirect, incidental or consequential damages or liability, under or in connection with or arising out of this tender and subsequent agreement or

services provided. The bidder should ensure that the due diligence and verification of antecedents of employees/personnel deployed by him for execution of this contract are completed and is available for scrutiny by the Bank.

33. Information Ownership

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

34. Inspection, Audit, Review, Monitoring & Visitations

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

- a. Ensure that the Bank has the ability to access all books, records and information relevant to the outsourced activity available with the BIDDER. For technology outsourcing, requisite audit trails and logs for administrative activities should be retained and accessible to the Bank based on approved request.
- b. Provide the Bank with right to conduct audits on the BIDDER whether by its internal or external auditors, or by external specialist appointed to act on its behalf and to obtain copies of any audit or review reports and finding made on the service provider in conjunction with the services performed for the bank.
- c. Include clause to allow the reserve bank of India or persons authorized by it to access the bank's documents: records of transactions, and other necessary information given to you, stored or

processed by the BIDDER within a reasonable time. This includes information maintained in paper and electronic formats.

- d. Recognized the right of the reserve bank to cause an inspection to be made of a service provider of the bank and its books and account by one or more of its officers or employees or other persons. Banks shall at least on an annual basis, review the financial and operational condition of the BIDDER. Bank shall also periodically commission independent audit and expert assessment on the security and controlled environment of the BIDDER. Such assessment and reports on the BIDDER may be performed and prepared by Bank's internal or external auditors, or by agents appointed by the Bank.
- e. Any such audit shall be conducted expeditiously, efficiently, and at reasonable business hours after giving due notice to the Bidder which shall not be less than 10 days. The Bank shall not have access to the proprietary data of, or relating to, any other customer of Bidder, or a third party or Bidder's cost, profit, discount and pricing data. The audit shall not be permitted if it interferes with Bidder's ability to perform the services in accordance with the service levels, unless the Bank relieves Bidder from meeting the applicable service levels. The audit shall not be performed by any competitor of the Bidder. The auditor including regulatory auditor shall sign the confidentiality undertaking with the Bidder before conducting such audit.

Monitoring

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

Visitations

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

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

35. Information Security

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

36. Intellectual Property Rights

The Bidder claims and represents that it has obtained appropriate rights to provide the Deliverables upon the terms and conditions contained in this RFP. The Bank agrees and acknowledges that same as expressly provided in this RFP, all Intellectual Property Rights in relation to the Hardware, Software and Documentation and any adaptations, translations and derivative works thereof whether protectable as a copyright, trade mark, patent, trade secret design or otherwise, provided by the Bidder during, in connection with or in relation to fulfilling its obligations under this RFP belong to and shall remain a property of the Bidder or its licensor. During the Term of this Project and, if applicable, during the Reverse Transition Period, Bank grants Bidder a right to use at no cost or charge the Hardware and Software licensed to the Bank, solely for the purpose of providing the Services. The Bidder shall be responsible for obtaining all necessary authorizations and consents from third party licensors of Hardware and Software used by Bidder in performing its obligations under this Project. If a third party's claim endangers or disrupts the Bank's use of the Hardware and Software, the Bidder shall at no further expense, charge, fees or costs to the Bank, (i) obtain a license so that the Bank may continue use of the Software in accordance with the terms of this tender and subsequent Agreement and the license agreement; or (ii) modify the Software without affecting the functionality of the Software in any manner so as to avoid the infringement; or (iii) replace the Software with a compatible, functionally equivalent and non-infringing product. All third party Hardware/software / service/s provided by the bidder in the scope of the RFP will be the responsibility of the bidder if any discrepancy or infringement is encountered. The Bank shall not be held liable for and is absolved of any responsibility or claim/Litigation or penal liability arising out of the use of any third party software or modules supplied by the Bidder as part of this Project.

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

exchange, mortgage, pledge, license, sub license, assign or in any other way convey, transfer or alienate the Bidder Pre-Existing IP in favour of any person (either for commercial consideration or not (including by way of transmission), and/or (c) except as specifically and to the extent permitted by the Bidder in the relevant Statement of Work, reverse compile or in any other way arrive at or attempt to arrive at the source code of the Bidder Pre-Existing IP.

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

37. Termination

Termination for Default

The Bank, without prejudice to any other remedy for breach of contract, by 30 (Thirty) days written notice of default sent to the Successful Bidder, may terminate this Contract in whole or in part:

- a. if the Successful Bidder fails to deliver any or all of the deliverables / milestones within the period(s) specified in the Contract, or within any extension thereof granted by the Bank provided the failure is for the reasons which are solely and entirely attributable to the Bidder and not due to reasons attributable to Bank and/or its other vendors or due to reasons of Force Majeure; or;
- b. If the Successful Bidder fails to perform any other material obligation(s) under the contract provided the failure is for the reasons which are solely and entirely attributable to the Bidder and not due to reasons attributable to Bank and/or its other vendors or due to reasons of Force Majeure.
- c. If the Successful Bidder, in the judgment of the Bank has engaged in corrupt or fraudulent practices in competing for or in executing the Contract.

Prior to providing a written notice of termination to the Selected Bidder, Bank shall provide the selected bidder with a written notice of 30 days to cure any breach of the Contract. The decision to terminate the contract shall be taken only if the breach continues or remains unrectified, for reasons within the control of Bidder, even after the expiry of the cure period.

In case the contract is terminated then all undisputed payment for the services delivered till the date of termination will be given to vendor, but disputed payment shall be discussed and will be paid once the dispute is resolved.

Termination for Insolvency

If either party becomes bankrupt or insolvent, has a receiving order issued against it, with its creditors, or, a resolution is passed or order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over any part of its undertaking or assets, or if either party takes or suffers any other analogous action in consequence of debt; then other party plans to, at any time, terminate the contract by giving written notice of 60 days to the party becoming bankrupt etc. If the contract is terminated by either party in terms of this

Clause, Bank shall be liable to make payment of the entire amount due under the contract for which services have been rendered by the Selected Bidder.

Termination- Key Terms & Conditions

Notwithstanding anything contain in this RFP, the Bank shall entitled to terminate the agreement with the service provider without assigning any reason at any time by giving 30 days prior written notice to the successful bidder . Bidder shall have to comply the same.

Either Party shall also be entitled to terminate the agreement at any time by giving notice if the other party.

- i. has a winding up order made against it; or
- ii. has a receiver appointed over all or substantial assets; or
- iii. is or becomes unable to pay its debts as they become due; or
- iv. enters into any arrangement or composition with or for the benefit of its creditors; or
- v. Passes a resolution for its voluntary winding up or dissolution or if it is dissolved.

Exit Option & Contract Re-Negotiation

The Bank reserves the right to cancel the contract in the event of happening one or more of the following Conditions:

- i. Failure of the successful bidder to accept the contract and furnish the Performance Guarantee within 21 days of receipt of purchase contract
- ii. Substantial delay in delivery, performance or implementation of the solution beyond the specified period.
- iii. Serious discrepancy in functionality to be provided or the performance levels agreed upon, which have an impact on the functioning of The Bank. Inability of the Bidder to remedy the situation within 60 days from the date of pointing out the defects by The Bank. (60 days will be construed as the notice period)

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

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

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

38. Privacy & Security Safeguards

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

39. Governing Law and Jurisdiction

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

Statutory and Regulatory Requirements

The solution must comply with all applicable requirements defined by any regulatory, statutory or legal body which shall include but not be limited to RBI or other Regulatory Authority, judicial courts in India and as of the date of execution of Agreement. This requirement shall supersede the responses provided by the Bidder in the technical response. During the period of warranty / AMC, Bidder / Bidder should comply with all requirements including any or all reports without any additional cost, defined by any regulatory authority time to time and which fall under the scope of this RFP / Agreement. All mandatory requirements by regulatory / statutory bodies will be provided by the bidder under change management at no extra cost to the bank during the tenure of the contract.

40. Compliance with Laws

1. Compliance with all applicable laws: Successful bidder shall undertake to observe, adhere to, abide by, comply with the Bank about all laws in force or as are or as made applicable in future, pertaining to or applicable to them, their business, their employees or their obligations towards them and all purposes of this scope of work.
2. Compliance in obtaining approvals/permissions/licenses: Bidder shall promptly and timely obtain all such consents, permissions, approvals, licenses, etc., as may be necessary or required for any of the purposes of this project or for the conduct of their own business under any applicable Law, Government Regulation/Guidelines and shall keep the same valid and in force during the term of the project.
3. The Annual Technical Support under the RFP should comply with all the Regulatory/ Compliance guideline of the Banks/ Regulatory authority in India. Bank has right to change the compliance/ guideline at any point of time and the service provider has to comply with the guidelines. Bank has right to audit by regulatory authority or any agency appointed by

the Bank, as a part of Vendor Audit. The service should comply with Bank IT/ Information Security (IS) / BCP Policy. It will be mandatory to protect the data privacy, as per Indian Data Privacy Law. Service provider should comply with all such laws in existence currently or introduced in future by the Govt. agencies or any other regulatory body.

41. Violation of Terms

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

42. Corrupt & Fraudulent Practices

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

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

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

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

43. Publicity

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

44. Entire Agreement; Amendments

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

45. Survival and Severability

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

Bidding Document

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

46. Amendments to Bidding Documents

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

47. Period of Validity

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

48. Ownership, Grant and Delivery

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

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

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

49. Last Date and Time for Submission of Bids

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

50. Late Bids

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

51. Modifications and/or Withdrawal of Bids

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

Clarification of Bids

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

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

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

52. Signing of Contract

The successful bidder(s) to be called as bidder, shall be required to enter into an Agreement with the Bank, within 21 days of the award of the work order (when provided) or within such extended period as may be specified by the bank. In case of inconsistency among the concerned RFP, this SLA and the Purchase order, the RFP clauses shall prevail.

53. Checklist for Submission

#	Particulars	Bidders Yes/No	Remark
1	Certificate of incorporation		
2	GSTN Registration Certificate		
3	Audited Balance sheets of last three years 2021-22, 2022-23 & 2023-24.		
4	CA certificate for three years average turnover for financial years 2021-22, 2022-23 & 2023-24.		
5	CA certificate for operating profit for last three financial years 2021-22, 2022-23 & 2023-24.		
6	CA certificate for net worth for last three financial years 2021-22, 2022-23 & 2023-24.		
7	Self-declaration on Company's letter head should not have been Blacklisted /debarred/ by any Govt. / IBA/RBI/PSU /PSE/ or Banks, Financial institutes for any reason or non-implementation/ delivery of the order. Self-declaration to that effect should be submitted along with the technical bid.		
8	Self-declaration on Company's letter head Bidder/OEM should not have any pending litigation or any dispute in the last five years, before any court of law between the Bidder or OEM and the Bank regarding supply of goods/services.		
9	Self-declaration by the Authorized Signatory for not have filed for bankruptcy in any country including India on company letter head		
10	Self-declaration on Company's letter-head for not having <ul style="list-style-type: none"> NPA with any Bank /financial institutions in India Any case pending or otherwise, with any organization across the globe which affects the credibility of the Bidder in the opinion of Central Bank of India to service the needs of the Bank Pending 		
11	Self-declaration by the Authorized Signatory for having support / service center or having support arrangement in Mumbai and Hyderabad.		
12	Reference Letters / Purchase Orders for Eligibility Criteria 11		
13	Reference Letters / Purchase Orders for Eligibility Criteria 12		
14	Annexure 1: Bill of Material		
15	Annexure 2: Minimum Technical Specifications		
16	Annexure 3: Conformity Letter		
17	Annexure 4: Masked Commercial Bid along with technical bid		
18	Annexure 5: Bidder's Information on company letter head		
19	Annexure 6: Letter for Conformity of Product as per RFP		
20	Annexure 7: Undertaking for acceptance of terms of RFP		
21	Annexure 8: MAF on OEM's letter head		

#	Particulars	Bidders Yes/No	Remark
22	Annexure 9: Integrity Pact		
23	Annexure 10: Non-Disclosure Agreement		
24	Annexure 11: Performance Bank Guarantee		
25	Annexure 12: Pro forma for Bid Security (EMD)		
26	Annexure 13: Bidders Particulars in Company Letter Head		
27	Annexure 14: NPA UNDERTAKING		
28	Annexure 15: Undertaking letter (Land Border Sharing)		
29	Annexure 16: Cover Letter		
30	Annexure 17: Pre-Bid Query Format		
31	Annexure 18: Eligibility Criteria Compliance		
32	Annexure 19: Guidelines on banning of business dealing		
33	Annexure 20: Compliance Certificate with respect to RBI's "Master Direction on Outsourcing of Information Technology Services"		

54. Annexure 1: Bill of Material

Format for Commercial Bill of Material is attached herewith :

COMMERCIAL BILL OF MATERIAL	
Instructions	
S.No.	Guidelines
I	Summary of Total Cost
1	The bidder is expected to quote the costs for all items required for fully complying with the requirements of the RFP and the corrigendum in the respective sections of the price bid. The prices for the respective sections would be deemed to include all components required to successfully utilise the solution.
2	Bank is not responsible for any arithmetic errors in the commercial bid details sheet committed by the bidders. All formulas & arithmetical calculations will be Vendor's responsibility.
3	The bidder is expected to specify the type of licences along with the details with respect to quantity, rate, etc., wherever applicable.
4	In case the bidder includes/combines any line item as part of any other line item in the commercial bid, then this has to be clearly mentioned in the description indicating the line item which contains the combination
5	The bidder has to quote for each line item. If any line item is part of the solution proposed in the RFP response, it has to be referenced. If it is not applicable, then the Bidder has to mention Not Applicable (NA).
6	The Bidder may insert additional line items as applicable based on the solution offered in the respective tabs
7	The Bidders should quote as per the format of Bill of Material ONLY and a masked replica of the Bill of Material should be enclosed in the technical bid.
8	Bidder is required to cover component by component licensing details for each of the software components proposed to the Bank
9	The <u>masked</u> Bill of Materials which would be submitted as part of the Technical Bill of Material should contain "XX" for ALL the corresponding commercial values that will be present in the unmasked Bill of Material that will be part of the Commercial submission.
10	All amounts in the Bill of Material should be in INR

11	The Bidder should to the extent possible stick to the same structure of the Bill of Material. Hence, the bidder is not expected to delete necessary rows.
12	All the prices quoted by the bidder shall be exclusive of taxes
13	Any additional number of items (software, hardware) and services to be procured by the Bank in future shall be on pro-rata basis on the rates provided in the Bill of Material.
14	If the bidder has not quoted for any line item mentioned in the Bill of Material, it will deemed considered that bidder has factored the cost for the item in the Bill of Material and No Additional charges will be paid other than the one mentioned in the Bill of Material .
15	Bidder is required to submit the indicative commercials during the bid submission and is required to provide the line item wise detailed breakup post reverse auction (RA)
II	Software
1	The bidder has to quote for each line item. If any line item is part of the solution proposed in the RFP response, it has to be referenced. If it is not applicable, then the Bidder has to mention Not Applicable (NA).
2	The Bidder can insert additional line items as applicable based on the solution offered in the various tabs
3	The license type , edition and version of the Software has to be clearly described in the Description column
4	The Bidder shall provide the maintenance (Warranty & ATS) for entire contract period.
III	Hardware, OS, DB & Peripheral
1	The bidder has to quote for each line item. If any line item is part of the solution proposed in the RFP response, it has to be referenced. If it is not applicable, then the Bidder has to mention Not Applicable (NA).
2	The Bidder can insert additional line items as applicable based on the solution offered in the various tabs
3	The Bidder shall provide the maintenance (Warranty, AMC & ATS) for the entire contract period.
4	The bidder is required to supply implement and maintain the hardware & associated software required for the solution.

IV	Installation & Implementation
1	Bidder shall comply to the Installation & commissioning, implementation scope provided in the RFP
2	Bidder shall provide the solution wise implementation cost. Each solution implementation should include all the costs associated with the complete implementation of the solution covering all the locations & implementation of associated components like software etc.
3	Activities and functions to be undertaken for installation and implementation of the licensed software should be as per the RFP.
V	ATS & Others, FM-Manpower
1	Bidder is expected to provide a detailed break up of all products and services that are under the scope of facilities management as part of the technical bid, in the technical bill of materials i.e. the above format is expected to be replicated for each item to be covered under the scope of facilities management.
2	The ATS costs for Production DC & DR, testing, development and training environments have to be quoted separately
3	The ATS cost for applications has to be quoted as separate line items in this section. If required, the Bidder has to create additional line items in this section.
4	Bidders must note that any Warranty pertaining to Software/Applications that extends beyond the contract period due to the Software/Applications supply towards the terminal years of the contract must be provided and supported by the Bidder without any additional cost to the Bank.
5	The Bidder needs to provide facility management services as per the scope of the RFP
6	The Bidder to provide FM resources as per the scope of the RFP
VI	Training
1	The rates provided by the bidders should be applicable for any additional training that the Bank may require throughout the tenure of the contract (on pro-rate basis).



RFP for Supply, Installation and Maintenance of
Cybersecurity Solutions and Associated
Hardware at the Bank

Summary of Total Cost

S.No	Items	Year 1	Year 2	Year 3	Year 4	Year 5	Total Amount for 5 years (in INR)
1	Software Cost	XX					XX
2	Hardware Cost	XX	XX	XX			XX
3	Installation & Commissioning Cost	XX					XX
4	AMC & ATS Cost		XX	XX	XX	XX	XX
5	FMS Cost	XX	XX	XX	XX	XX	XX
6	Professional Services Cost	XX	XX	XX	XX	XX	XX
	Grand Total - TCO						XX

****All the prices quoted by the bidder shall be exclusive of taxes**

The Cost should flow from the respective sheets

Total Cost in Words:

Software Cost

S. No	Software (license) Cost at DC	Description (OEM Name, Solution Name, Version, Edition, Licensing Metrics)	YEAR 1			YEAR 2			YEAR 3			YEAR 4			YEAR 5			Total Amount for 5 years (INR)
			Quantity	Rate (INR)	Total Amount (INR)	Quantity	Rate (INR)	Total Amount (INR)	Quantity	Rate (INR)	Total Amount (INR)	Quantity	Rate (INR)	Total Amount (INR)	Quantity	Rate (INR)	Total Amount (INR)	
1	Data Discovery & Classification			XX	XX													XX
2	File Upload Security Solution			XX	XX													XX
3	Attack Surface Management (ASM)			XX	XX													XX
4	Breach and Attack Simulation (BAS) with Red Team Solution			XX	XX													XX
5	Phishing Simulation			XX	XX													XX

6	AD Security			XX	XX														XX
7	Governance, Risk and Compliance			XX	XX														XX
8	Decoy (Honeypot)			XX	XX														XX
9	Mobile Device Management			XX	XX														XX
10	Secure Data Backup and Recovery (Ransomware Solution)			XX	XX														XX
11	Network Access Control (NAC)			XX	XX														XX
	Any other (Please specify)			XX	XX														XX
	Any other (Please specify)			XX	XX														XX
	Total (A)			XX	XX														XX
S. No	Software (license) Cost at DRC	Description (OEM Name, Solution Name, Version, Edition,	Quantity	Rate (INR)	Total Amount (INR)	Quantity	Rate (INR)	Total Amount (INR)	Quantity	Rate (INR)	Total Amount (INR)	Quantity	Rate (INR)	Total Amount (INR)	Quantity	Rate (INR)	Total Amount (INR)	Total Amount for 5 years (INR)	

RFP for Supply, Installation and Maintenance of
Cybersecurity Solutions and Associated
Hardware at the Bank

		Licensi ng Metrics)																		
1	Data Discovery & Classification			XX	XX															XX
2	File Upload Security Solution			XX	XX															XX
3	Attack Surface Management (ASM)			XX	XX															XX
4	Breach and Attack Simulation (BAS) with Red Team Solution			XX	XX															XX
5	Phishing Simulation			XX	XX															XX
6	AD Security			XX	XX															XX
7	Governance, Risk and Compliance			XX	XX															XX
8	Decoy (HoneyPot)			XX	XX															XX
9	Mobile Device Management			XX	XX															XX
10	Secure Data Backup and Recovery (Ransomware Solution)			XX	XX															XX
11	Network Access Control (NAC)			XX	XX															XX

RFP for Supply, Installation and Maintenance of
Cybersecurity Solutions and Associated
Hardware at the Bank

	Any other (Please specify)			XX	XX														XX	
	Any other (Please specify)			XX	XX															XX
	Total (B)			XX	XX															XX
	Grand Total (A+B)			XX	XX															XX

Hardware Cost

S. No	Hardware Cost at DC	Details of the proposed hardware (Make, Model, etc)	YEAR 1			YEAR 2			YEAR 3			YEAR 4			YEAR 5			Total Amount for 5 years (INR)
			Quantity	Rate (INR)	Total Amount (INR)	Quantity	Rate (INR)	Total Amount (INR)	Quantity	Rate (INR)	Total Amount (INR)	Quantity	Rate (INR)	Total Amount (INR)	Quantity	Rate (INR)	Total Amount (INR)	
1	Data Discovery & Classification			XX	XX		XX	XX		XX	XX							XX
2	File Upload Security Solution			XX	XX		XX	XX		XX	XX							XX
3	Attack Surface Management (ASM)			XX	XX		XX	XX		XX	XX							XX
4	Breach and Attack Simulation (BAS) with Red Team Solution			XX	XX		XX	XX		XX	XX							XX
5	Phishing Simulation			XX	XX		XX	XX		XX	XX							XX
6	AD Security			XX	XX		XX	XX		XX	XX							XX
7	Governance, Risk and Compliance			XX	XX		XX	XX		XX	XX							XX

RFP for Supply, Installation and Maintenance of
Cybersecurity Solutions and Associated
Hardware at the Bank

8	Decoy (Honeypot)			XX	XX		XX	XX		XX	XX							XX
9	Mobile Device Management			XX	XX		XX	XX		XX	XX							XX
10	Secure Data Backup and Recovery (Ransomware Solution)			XX	XX		XX	XX		XX	XX							XX
11	Network Access Control (NAC)			XX	XX		XX	XX		XX	XX							XX
	Any Other (Please specify)			XX	XX		XX	XX		XX	XX							XX
	Any Other (Please specify)			XX	XX		XX	XX		XX	XX							XX
	Total Software Cost (A)			XX	XX		XX	XX		XX	XX							XX
S. No	Hardware Cost at DRC	Details of the proposed hardware (Make, Model, etc)	Quantity	Rate (INR)	Total Amount (INR)	Quantity	Rate (INR)	Total Amount (INR)	Quantity	Rate (INR)	Total Amount (INR)	Quantity	Rate (INR)	Total Amount (INR)	Quantity	Rate (INR)	Total Amount (INR)	Total Amount for 5 years (INR)

RFP for Supply, Installation and Maintenance of
Cybersecurity Solutions and Associated
Hardware at the Bank

1	Data Discovery & Classification			XX	XX		XX	XX		XX	XX									XX
2	File Upload Security Solution			XX	XX		XX	XX		XX	XX									XX
3	Attack Surface Management (ASM)			XX	XX		XX	XX		XX	XX									XX
4	Breach and Attack Simulation (BAS) with Red Team Solution			XX	XX		XX	XX		XX	XX									XX
5	Phishing Simulation			XX	XX		XX	XX		XX	XX									XX
6	AD Security			XX	XX		XX	XX		XX	XX									XX
7	Governance, Risk and Compliance			XX	XX		XX	XX		XX	XX									XX
8	Decoy (Honey-pot)			XX	XX		XX	XX		XX	XX									XX
9	Mobile Device Management			XX	XX		XX	XX		XX	XX									XX
10	Secure Data Backup and Recovery (Ransomware Solution)			XX	XX		XX	XX		XX	XX									XX
11	Network Access Control (NAC)			XX	XX		XX	XX		XX	XX									XX
	Any Other (Please specify)			XX	XX		XX	XX		XX	XX									XX

RFP for Supply, Installation and Maintenance of
Cybersecurity Solutions and Associated
Hardware at the Bank

	Any Other (Please specify)			XX	XX		XX	XX		XX	XX							XX
	Total Software Cost (B)			XX	XX		XX	XX		XX	XX							XX
	Grand Total (A+B)			XX	XX		XX	XX		XX	XX							XX

Note

Bidders have to specify the particulars including the configurations for the listed solutions as per their solution design to meet the requirements of the RFP
Bidder to clearly specify the description of all proposed software, Bank may procure the software based on the rate provided on pro-rata basis.
The Hardware costing should be inclusive of OS



RFP for Supply, Installation and Maintenance of
Cybersecurity Solutions and Associated
Hardware at the Bank

Installation and Implementation Cost

Production Environment					
Installation and Commissioning Cost at DC					
S. No	Installation & Commissioning at DC	Quantity	Rate (INR)	Total Amount (INR)	Total Amount for 5 yrs (INR)
1	Data Discovery & Classification		XX	XX	XX
2	File Upload Security Solution		XX	XX	XX
3	Attack Surface Management (ASM)		XX	XX	XX
4	Breach and Attack Simulation (BAS) with Red Team Solution		XX	XX	XX
5	Phishing Simulation		XX	XX	XX
6	AD Security		XX	XX	XX
7	Governance, Risk and Compliance		XX	XX	XX
8	Decoy (Honey-pot)		XX	XX	XX
9	Mobile Device Management		XX	XX	XX
10	Secure Data Backup and Recovery (Ransomware Solution)		XX	XX	XX
	Any other (Please specify)		XX	XX	XX
	Any other (Please specify)		XX	XX	XX
	Total (A)		XX	XX	XX
Installation and Commissioning Cost at DRC					
S. No	Installation & Commissioning at DRC	Quantity	Rate (INR)	Total Amount (INR)	Total Amount for 5 yrs (INR)
1	Data Discovery & Classification		XX	XX	XX
2	File Upload Security Solution		XX	XX	XX
3	Attack Surface Management (ASM)		XX	XX	XX
4	Breach and Attack Simulation (BAS) with Red Team Solution		XX	XX	XX

RFP for Supply, Installation and Maintenance of
Cybersecurity Solutions and Associated
Hardware at the Bank

5	Phishing Simulation		XX	XX	XX
6	AD Security		XX	XX	XX
7	Governance, Risk and Compliance		XX	XX	XX
8	Decoy (Honeypot)		XX	XX	XX
9	Mobile Device Management		XX	XX	XX
10	Secure Data Backup and Recovery (Ransomware Solution)		XX	XX	XX
11	Network Access Control (NAC)		XX	XX	XX
	Any other (Please specify)		XX	XX	XX
	Any other (Please specify)		XX	XX	XX
	Total (B)		XX	XX	XX
	Grand Total (A+B)		XX	XX	XX



RFP for Supply, Installation and Maintenance of
Cybersecurity Solutions and Associated
Hardware at the Bank

RFP for Supply, Installation and Maintenance of
Cybersecurity Solutions and Associated
Hardware at the Bank

Production Environment																	
		YEAR 1			YEAR 2			YEAR 3			YEAR 4			YEAR 5			Total Amount
S. No	AMC / ATS at DC	Base Product Cost	Rate (INR)	Total Amount (INR)	Base Product Cost	Rate (INR)	Total Amount (INR)	Base Product Cost	Rate (INR)	Total Amount (INR)	Base Product Cost	Rate (INR)	Total Amount (INR)	Base Product Cost	Rate (INR)	Total Amount (INR)	Total Amount for 5 years (INR)
1	Data Discovery & Classification																
	AMC										XX	XX	XX	XX	XX	XX	XX
	ATS				XX	XX	XX	XX									
2	File Upload Security Solution																
	AMC										XX	XX	XX	XX	XX	XX	XX
	ATS				XX	XX	XX	XX									
3	Attack Surface Management (ASM)																
	AMC										XX	XX	XX	XX	XX	XX	XX
	ATS				XX	XX	XX	XX									
4	Breach and Attack Simulation																

RFP for Supply, Installation and Maintenance of
Cybersecurity Solutions and Associated
Hardware at the Bank

	(BAS) with Red Team Solution																
	AMC									XX	XX						
	ATS				XX	XX											
5	Phishing Simulation																
	AMC									XX	XX						
	ATS				XX	XX											
6	AD Security																
	AMC									XX	XX						
	ATS				XX	XX											
7	Governance, Risk and Compliance																
	AMC									XX	XX						
	ATS				XX	XX											
8	Decoy (Honey pot)																
	AMC									XX	XX						
	ATS				XX	XX											
9	Mobile Device Management																
	AMC									XX	XX						
	ATS				XX	XX											
10	Secure Data																

RFP for Supply, Installation and Maintenance of
Cybersecurity Solutions and Associated
Hardware at the Bank

	Backup and Recovery																
	AMC										XX	XX	XX	XX	XX	XX	XX
	ATS				XX	XX	XX	XX									
11	Network Access Control (NAC)																
	AMC										XX	XX	XX	XX	XX	XX	XX
	ATS				XX	XX	XX	XX									
	Any other, please specify																
	AMC										XX	XX	XX	XX	XX	XX	XX
	ATS				XX	XX	XX	XX									
	Any other, please specify																
	AMC										XX	XX	XX	XX	XX	XX	XX
	ATS				XX	XX	XX	XX									
	TOTAL (A)																
		YEAR 1			YEAR 2			YEAR 3			YEAR 4			YEAR 5			
	AMC / ATS at DRC	Base Product Cost	Rate (INR)	Total Amount (INR)	Base Product Cost	Rate (INR)	Total Amount (INR)	Base Product Cost	Rate (INR)	Total Amount (INR)	Base Product Cost	Rate (INR)	Total Amount (INR)	Base Product Cost	Rate (INR)	Total Amount (INR)	Total Amount for 5 years (INR)

1	Data Discovery & Classification																	
		AMC									XX							
		ATS			XX													
2	File Upload Security Solution																	
		AMC									XX							
		ATS			XX													
3	Attack Surface Management (ASM)																	
		AMC									XX							
		ATS			XX													
4	Breach and Attack Simulation (BAS) with Red Team Solution																	
		AMC									XX							
		ATS			XX													
5	Phishing Simulation																	
		AMC									XX							
		ATS			XX													

6	AD Security																
	AMC									XX							
	ATS				XX												
7	Governance, Risk and Compliance																
	AMC									XX							
	ATS				XX												
8	Decoy (Honeypot)																
	AMC									XX							
	ATS				XX												
9	Mobile Device Management																
	AMC									XX							
	ATS				XX												
10	Secure Data Backup and Recovery																
	AMC									XX							
	ATS				XX												
11	Network Access Control (NAC)																

FMS Cost

Description	YEAR 1			YEAR 2			YEAR 3			YEAR 4			YEAR 5			Total Amount for 5 years (INR)
	No. of Resources	Rate per resource (INR)	Total Amount (INR)	No. of Resources	Rate per resource (INR)	Total Amount (INR)	No. of Resources	Rate per resource (INR)	Total Amount (INR)	No. of Resources	Rate per resource (INR)	Total Amount (INR)	No. of Resources	Rate per resource (INR)	Total Amount (INR)	
L1 Resource	8	XX	XX	XX												
L2 Resource	2	XX	XX	XX												
Any Other (Please specify)		XX	XX	XX												
Any Other (Please specify)		XX	XX	XX												
Grand Total																

Note:

1. Bidder is required to right size the resources deployment (L1 and L2) in order to meet the project timelines, SLA and Scope of the RFP

Professional Services

Professional Services Cost over the period of 5 Years												
Sl.No		Year 1		Year 2		Year 3		Year 4		Year 5		Total
		No. of Mandays (M) / Hours (H)	Cost	No. of Mandays	Cost							
1	Data Discovery & Classification	XX		XX		XX		XX		XX		-
2	File Upload Security Solution	XX		XX		XX		XX		XX		-
3	Attack Surface Management (ASM)	XX		XX		XX		XX		XX		-
4	Breach and Attack Simulation (BAS) with Red Team Solution	XX		XX		XX		XX		XX		-
5	Phishing Simulation	XX		XX		XX		XX		XX		-
6	AD Security	XX		XX		XX		XX		XX		-
7	Governance, Risk and Compliance	XX		XX		XX		XX		XX		-
8	Decoy (Honey-pot)	XX		XX		XX		XX		XX		-
9	Mobile Device Management	XX		XX		XX		XX		XX		-
10	Secure Data Backup and Recovery (Ransomware Solution)	XX		XX		XX		XX		XX		-
11	Network Access Control (NAC)	XX		XX		XX		XX		XX		-

				TOTAL	-
Additional Professional Services Cost over the period of for 5 Years					
		5 Years			Total
	No. of Mandays	Cost for 5 Years *			
	Additional Professional Service Man-days for the period of 5 years		Additional Professional Service Hours is for the purpose of TCO. However, Bank will pay on actuals as per usage of mandays. Additional Professional Services will be used on fully utilisation of yearly Professional Services.		
1	Data Discovery & Classification	XX (M)			-
2	File Upload Security Solution	XX (M)			-
3	Attack Surface Management (ASM)	XX (M)			-
4	Breach and Attack Simulation (BAS) with Red Team Solution	XX (M)			-
5	Phishing Simulation	XX (M)			-
6	AD Security	XX (M)			-
7	Governance, Risk and Compliance	XX (M)			-
8	Decoy (Honeypot)	XX (M)			-
9	Mobile Device Management	XX (M)			
10	Secure Data Backup and Recovery (Ransomware Solution)	XX (M)			
11	Network Access Control (NAC)	XX (M)			

55. Annexure 2: Minimum Technical Specifications

Format for Minimum Technical Specifications is attached herewith :

Technical Specifications for Data Discovery and Classification			
S No	Minimum Technical Specifications	Vendor's Compliance	Vendor's Remark
A	Automated Data Discovery		
1	The solution must provide automated data discovery capabilities across various data repositories, including on-premises storage, cloud storage, and databases.		
2	The solution should be able to scan and identify structured and unstructured data within and across Bank's environment, including multi cloud environment.		
3	The system must offer scheduling options for regular data discovery scans to ensure up-to-date data inventory and preferably also provide real-time alerts for newly discovered sensitive data.		
4	The solution should support data discovery handling of complex & customized data objects		
5	The solution should support automated data identification of simple and complex data types		
B	Multi-factor Data Classification		
4	The platform should employ a multi-factor approach to data classification, considering content, context, and user-defined criteria along with the Support for machine learning models to improve classification accuracy over time.		
5	It must support both automated and manual classification methods, allowing for human oversight and input where necessary and preferably should allow integration with third-party AI tools for enhanced classification.		
6	The solution should support categorization and sub-categorization levels of data objects classification		
7	The solution should offer pre-defined classification templates based on common regulatory requirements (e.g., GDPR, PCI-DSS, Regulatory compliances etc), with the ability to customize these templates.		

C	Content-based Classification		
7	Include "The system must use pattern matching and regular expressions to identify sensitive data types such as credit card numbers, social security numbers (Ex. Aadhar Card , PAN Card, BIN numbers etc.), and email addresses and should support advanced pattern recognition, including custom regex and preferably also the AI-driven context analysis."		
8	It should incorporate natural language processing capabilities to understand the context and sensitivity of unstructured text data and preferably also support multilingual data classification.		
9	The solution must be able to recognize and classify images containing sensitive information, such as scanned documents or IDs.		
D	Metadata Analysis		
10	The platform should analyze file metadata to aid in classification, including factors such as file type, creation date, and access permissions and preferably should provide insights into data retention policies based on metadata.		
11	It must be able to track data lineage and classify data based on its source or movement within the organization.		
E	Customizable Classification Policies		
12	The solution must allow organizations to define and implement custom classification policies based on their specific needs and risk profile.		
13	It should support the creation of hierarchical classification levels (e.g., Public, Internal, Confidential, Restricted, secret, top secret etc) with clear definitions and handling rules for each level.		
F	Classification Consistency		
14	The system must maintain consistent classification across different storage locations and data formats.		
15	It should provide mechanisms to resolve conflicts in classification, especially when data is moved or copied between locations.		
G	User Friendly Classification Interface		
16	The platform must offer a user-friendly interface for manual classification, allowing authorized users to easily review and classify data.		

17	It should provide options for bulk classification to efficiently handle large volumes of similar data.		
H	Integration with Access Control Systems		
18	The solution must be able to integrate with existing access control systems to enforce data access based on classification levels.		
19	It should support the automatic application of security controls (e.g., encryption, access restrictions) based on data classification.		
I	Audit and Reporting		
20	The system must maintain a detailed audit trail of all classification activities, including automated classifications and manual overrides.		
21	It should offer customizable reports on data classification status, distribution of data across classification levels, and potential misclassifications.		
J	Continuous Monitoring and Reclassification		
22	The platform should continuously monitor classified data for changes that might affect its classification status preferably with AI-driven predictive analysis to foresee potential classification changes.		
23	It must support automated reclassification based on predefined rules or changes in data content or context.		
K	Data Visualization		
24	The solution should provide visual representations of classified data distribution across the organization's environment.		
25	It must offer interactive dashboards to help stakeholders understand the overall data classification landscape.		
26	The solution should provide options to display both graphical visualization as well as a statistical visualization of the data maps		
L	Performance and Scalability		
26	The system must be designed to handle large volumes of data without significant impact on network or storage system performance and should provide resource usage analytics to optimize performance.		
27	It should offer options for incremental scanning and classification to manage resource utilization effectively.		
M	General System Requirements		

	Scalability and Performance:		
28	The solution platform must be scalable to accommodate organization's current and future security needs.		
29	The solution should ensure high performance ingestion and low latency inference, even under heavy load conditions such as 10k events/second.		
30	The solution provider should have proven scalability benchmarks and validated performance metrics in industry-standard benchmarks including validated presence in open leaderboard		
	High Availability and Disaster Recovery:		
31	The solution should provide automated high availability and disaster recovery capabilities to ensure continuous security operations.		
32	The solution should support redundant infrastructure and automated failover mechanisms.		
	Security and Compliance:		
33	The solution should meet industry security standards and best practices for data protection and access control.		
34	The solution should comply with relevant regulations and compliance frameworks, such as PCI DSS, Data Protection Related Regulations from the RBI, Govt of India and provide automated compliance reporting.		
	Open Integration and Extensibility:		
35	The solution should adhere to open integration standards and APIs for seamless integration with third-party tools and systems using RestAPI.		
36	The solution should provide a flexible framework for developing custom connectors and extensions.		
	Other Features		
37	The Solution should perform Data Discovery and Classification with office tools from Microsoft.		
38	The Solution should perform Data Discovery and Classification with standard email tools such as IBM Lotus, Office 365 etc.		
39	Solution should be able to scan compressed files, Image Files		
40	The solution should allow to classify files within the files when the file is open		

41	The solution should have the feature such that user is prompted to reclassify the file in case of changes made to the files		
42	The solutions should be integrated with DLP, SIEM		
43	The solution should Identify and categorize/develop inventory of sensitive data, PII, or any other critical data as the Bank's requirements		
44	The solution should Support for scanning all types of file formats like pdf, excel, ppt, word, text files, files without extensions		
45	The solution should Support to scan compressed files like zip, rar, 7z etc		
46	The solution should Support for scanning Image files with OCR		
47	The solution should Support for scanning images inside PDF, Document, PPT etc.,CAD - engineering drawings		
48	The solution should enable the classification of Word, Excel, PowerPoint, Open source office documents from within.		
49	The solution should enable user can define different Classification labels like public, internal, confidential, restricted etc.		
50	The solutions should be able to insert metadata tags in the documents and emails which can be read by DLP Solutions.		
51	The solution should be able to track initial classification and reclassification events at both document and central logging level.		
52	The solution should have the ability to classify based on context based on file attributes, ip, hostname, username etc. for example if finance team is creating a file with "shareholder_data" it should be classified as confidential.		
53	The solution should be able to blacklist domains for blocking emails originating out of email domain and also bind certain classification categories with a fixed domain name.		
54	The solution should trigger classification for document on Save, Save As, Print etc. and should be configurable using a management mechanism.		
55	The solution should trigger classification based on send, reply, forward emails.		
56	The solution should provide automated, suggestive and manual classification capability		
57	The solution should detect unclassified documents attached in an email and block the user the email.		

58	The solution should have some guidance mechanism while user selects a classification level, to inform the users what is the context of a said classification level as per organization's policy		
59	The solution should be capable to deploy and enforcing user based policies.		
60	The solution should further allow policies which are based on a combination of keywords and regular expressions. The solution should allow administrators to define own regex for adding capability to detect any new type of regex.		
61	The solution should suggest a classification based in content, but should allow user to change the classification if required by taking a justification for the same and recording it in logs.		
62	The solution should log user activity while users are handling email, documents, and files.		
63	The solution should have Manual, Automated and Suggested Classification feature		
64	The solution should have the ability to classify based on content like if Credit card or Aadhaar card is identified, tool should automatically classify file as restricted		
65	The solution should support display icons over files that have been classified using the solution.		
66	The solution should support hierarchical and conditional classification fields, so that the appearance of a sub-field is conditional on the value selected in the higher-level field. For example, when a user selects "Restricted," a sub-field is presented with a list of departments including "Office use", "Branch use", "HR Only" etc.		
67	The solution should support Open source office.		
68	The solution should integrate with DRM/IRM, SIEM, PIM/PAM, AD		

Technical Specifications for File Upload Security			
S No	Minimum Technical Specifications	Vendor's Compliance	Vendor's Remark
A	Solution Capabilities		
1	Solution should be able to integrate using API or ICAP for scanning files uploaded to web applications/SFTP		
2	The proposed solution must be on premise and capable to perform local analysis of the sample submissions with no analyzed data going outside Bank's infrastructure. However, solution should be cloud ready.		
3	The proposed solution should have the ability to perform the simulation of unknown code before the code is executed to determine malicious intent without requiring end-user interaction with the unknown code.		
3	The proposed solution shall be able to do unlimited number of file scans without any restriction		
3	The solution shall be software based appliance		
4	The solution should get integrated using REST API with the application and provide a detailed API response for the application to take an action on the file scanning verdict		
5	The Solutions shall support ICAP integration with standard security solutions like proxy /reverse proxy systems/next generation firewalls/web application firewalls/MFT's		
6	The solution shall support detection and extraction of standard archive file types, including (but not limited to) Microsoft Office documents, Zip, 7z, Jar, RAR, TAR, ISO, Gzip, APK, MSI, TGZ, TBZ, and BZ2 without any restriction on archive level, number of files & file size		
7	The solution shall support blacklisting and whitelisting based on hash, filename, file type and MIME type.		
8	The solution shall not send any files being scanned out of the solution or organization		
9	The solution should support multiple security rules for different applications based on Host,client or HTTP headers		
10	The solution should support HA / loadbalancing		
11	The solution should be able to detect & sanitize embedded objects and active content in the files.		
B	Detection & Protection Capabilities		
12	The Solution shall have multiple Anti-Virus/Malware (AM) Engines support from Globally leading Anti- malware companies. Minimum 5 different Anti- Virus/Malware engines shall be available in the solution to scan the files		
13	The solution shall use signature-based detection/heuristic based detection/machine learning based detection		

14	The multiple AV engines shall be able to run in a multithreaded parallel way reducing delay and resource overheads		
15	The frequency of the signature definition updates shall be configurable		
16	The solution shall be able to quarantine malicious sample for further analysis		
17	The solution must have option to enable/ disable/configure AV engines individually		
18	The solution shall provide a false positive configurable threshold.		
19	The solution shall be able to scan standard documents, images, pdf and archive files		
20	The solution shall offer configurable content disarm reconstruction, and file sanitization technology.		
21	The solution should be able to remove malicious embedded objects and provide a clean, sanitized file.		
22	The sanitization process shall provide detailed information on any removed & sanitized objects.		
23	After sanitization, the entire file shall be reconstructed to ensure safety and maintain full usability in the original file format		
24	The solution should be able to sanitize most common file types like .doc,.docx,.xls,.xlsx,.ppt,.pptx,.pdf,.jpg,.jpeg,.png,.rtf,.vsdx,htm,html,xml etc		
25	The solution should be able to do recursive sanitation of files in archives (zip,tar,rar,7z) without any limit on recursive archive level & child file. Also should sanitize files embedded into the files like docx,pptx,xlsx		
26	Solution should provide sandboxing of malicious or suspicious file locally		
27	Solution should have API interfaces for submitting files for sandboxing		
28	Sandbox Service should have be emulation based and should not spin up separate VM's for analysis		
	The proposed solution should support re-analysis of samples already processed if required.		
21	The proposed solution should be able to detect ransomware and advanced threats and detect multi-stage malicious downloads, outbound connections and command and control from malicious attachments and URLs.		
29	The proposed solution should support sharing of threat insight automatically with own solution components and third party products with open standards like STIX, TAXII etc		
30	The proposed solution should have ability to shares new IOC detection intelligence automatically with supported and third-party products		
31	The proposed solution shall have virtual environment that must be securely isolated from the rest of the network to avoid malware propagation.		
32	Sharable threat intelligence must include at least 4 types - IP, URL, domain, e-mail-ids and file checksum		

33	The proposed solution should be able to run multiple parallel sandboxes for analysis of payload and on premise customized file scanning solution should have the capability to allow manual submission of suspicious files for analysis.		
34	The proposed solution should be able to identify password-protected archive file or password-protecting document files by providing options to define a commonly used password list.		
35	The proposed solution should integrate with a Active Directory server to allow user accounts to be added to management console.		
18	The proposed solution should have a on-premises management solution for centralized deployment of hotfixes, critical patches, firmware, sandboxing virtual images or serve as threat intelligence sharing platform.		
19	The proposed solution should have a secure web based console that can display information such as risk level of submissions, processing time, number of processing samples etc.		
20	The proposed solution should support custom integration by sharing new IOC detection intelligence automatically with existing solutions and third-party products.		
C	Management & Reporting		
29	The solution shall integrate with syslog/SIEM systems		
30	The solution must support role-based access control		
31	The solution shall provide Active Directory and LDAP group-based administrative roles		
32	Solution shall have its logs archived locally, and they shall be downloadable via the GUI		
33	The solution shall allow configuration export and backup		
34	Web access to the platform shall be via https protocol.		
35	The solution should provide auditable record of files that has been scanned for RCA etc.		
36	The solution shall work in Air-gapped environment and support offline update of signatures		

Technical Specifications for Attack Surface Management			
S No	Minimum Technical Specifications	Vendor's Compliance	Vendor's Remark
1	The solution should offer frequent, high-quality internet indexing with proprietary technology and ensure result accuracy.		
2	The solution must generate its own scan data independently and avoid reliance on third-party providers.		
3	The solution should have a minimum of 3 years of experience in scanning the internet.		
4	The solution should perform rescans on a daily basis or at a faster frequency.		
5	The solution should support detection across more than 2500 common / widely used ports for comprehensive coverage.		
6	The solution should perform full protocol handshakes, rather than just open port checks, to ensure accuracy.		
7	The solution should crawl websites and provide detailed reports, including screenshots.		
8	The solution should fully support IPv4.		
9	The solution should fully support IPv6.		
10	The solution should identify various assets exposed to the global internet, including but not limited to:		
11	The solution should identify and discover IP ranges.		
12	The solution should identify certificates and provide a specific inventory view for them.		
13	The solution should identify paid-level domains.		
14	The solution should identify subdomains associated with the organization.		
15	The solution should identify and discover websites.		
16	The solution should include discovery of cloud compute instances.		
17	The solution should enumerate all services running on discovered assets.		
18	The solution should provide detailed contextual information for each asset type, including registration details.		
19	The solution should use machine learning for asset mapping, complemented by human analyst expertise for accuracy.		
20	The solution should enrich data to provide broader context and insights.		
21	The solution should include date and time information in scan results.		

22	The solution should incorporate GeolP data for enhanced contextual information.		
23	The solution should include Common Vulnerabilities and Exposures (CVE) data.		
24	The solution should not only identify but also assist in managing cloud assets.		
25	The solution should identify assets across all major cloud providers.		
26	The solution should treat dynamic assets in a simple manner, so that results can be de-duplicated when a single identifier is seen hosted many times across large CDNs		
27	The solution should distinguish between directly attributable assets and co-located services		
28	The solution should allow for the configuration of approved and unapproved cloud providers, and corresponding alerts		
29	Tooling to streamline the management of assets		
30	The solution should have a defined and scoped process for validating that assets do in fact belong to that organization		
31	The solution should describe why an asset is attributed to the Bank.		
32	The solution should label assets with an ownership confidence score		
33	The solution should provide visibility into assets across cloud providers, certificate issuers and domain registrars. Also, solution should provide contextual visibility into all assets by: <ul style="list-style-type: none"> • Criticality based on asset attribute and activity. • Graphical presentation on relationship of assets • Historical risk assessment result 		
34	The solution should highlight stale IP registration records for update and to reflect accurate ownership		
35	The solution should forecast all asset expirations including certificate and domain registrations for proactive maintenance.		
36	The ability to apply tags to enable advanced data filtering, customized data, and to restrict or permit access to data		
37	The solution should have Risk scoring and prioritization capabilities		
38	The solution should identify risks across Bank's assets, categorize the risk, and prioritize incidents for remediation		
39	Risk score should be based on accepted industry metrics, and allow for customization		
40	The solution should offer remediation guidance for risks		
41	The solution should group alerts impacting the same service together automatically		
42	The solution should be capable of actually fixing things		

43	The solution should have the ability to automate common actions. This includes pulling in known asset owners, sending automated emails, or automatically creating tickets for investigation.		
44	The solution should have the ability to automatically remediate exposures. This should include full resolution of the incident by reaching back via API and blocking the service at the port level.		
45	Allow customizability to the remediation path		
46	In platform instructions on how to set up integrations and use Automated Remediation		
47	A comprehensive score on Bank's overall security posture		
48	The solution should have the ability to allow users to customize the weight of incidents in their overall risk score based on the organizations needs		
49	The solution should update the score based on what new incidents are found and should not have delays in score updates		
50	Ability to create or remove risk scoring rules		
51	Ability to override the default system score and enter a score		
52	The solution should provide risk scoring using or leveraging a combination of CVSS (Common Vulnerability Scoring System) and EPSS (Exploit Prediction Scoring System) data		
53	The solution should have a method of explaining why an asset was attributed to the organization		
54	The solution should describe why the asset was attributed & provide evidence		
55	The solution should be explicit on how confident the product is on the attribution		
56	The solution should offer features that improve enterprise usability and function		
57	Supports single-sign on with Security Assertion Markup Language (SAML)		
58	Allows you to directly export any data from the platform		
59	Create dashboards based on the needs of Bank and based on what visibility Bank is looking to have.		
60	Create reports based on the needs of Bank and schedule regular reporting on a particular cadence for quicker reporting cycles		
61	Perform AND/OR searches across assets to drill down easily		
62	Allow for designated administrators to add, delete, and edit users		
63	Select from default roles or create new role with designated privileges for better security		
64	Create User Groups based on a role for quick administration		
65	The solution should come with integrations to other popular tools		

66	Stay in one platform to manage all API keys for integrations		
67	A central location for installing, exchanging, and managing of Bank's content including playbooks, integrations, automations, fields, layouts, etc.		
68	Connect to IT Asset Repository and ITSM to easily create new tickets based on incidents, identify the owner, and close out open ones.		
69	The solution should integrate with standard cloud service providers such as AWS, Azure, GCP etc. for greater visibility into cloud assets		
70	Supported integration into SIEM tools		
71	The solution should have integrations with a SOAR tool		
72	The solution should offer ways to manage compliance and standards		
73	Provide compliance dashboards that map identified Issues to compliance frameworks to help our teams understand their overall compliance with regulatory and organizational policies. These dashboards need to provide executive visibility, prioritize high-risk cybersecurity areas, and measure the progress of our organization's maturity.		
74	The solution should offer a way of managing assets and identifying risk through policies		
75	Provide accurate context & classification to enable automated policy development and mitigate security exposures identified.		
76	Identify all VPNs, certificates about to expire, domains about to expire, etc.		
77	The solution should identify potential vulnerabilities such as sites using word press plugins, ecommerce sites, analytic packages, blogs, and web frameworks in the Bank's internet-facing assets.		
78	A flexible policy engine that allows rapid building of new fingerprints and detect devices against critical CVEs		
79	Offer descriptions of common CVEs and the best practices around securing Bank's assets from them		
80	Built-in security policies and settings must:		
80.1	Enable the Bank to define the number of hours after which the user login session will expire.		
80.2	Enable the Bank to define approved domains and approved IP ranges through which access the platform		
80.3	Enable the Bank to specify one or more domain names that can be used in Bank's distribution lists		
80.4	Enable the Bank to deactivate an inactive user & set a deactivation time period		
81	Provide risk assessment for each domain and IP address asset and assign a risk score that can be monitored over time. Display risk indicators like what type of risks, events, and risk level for each discovered risk.		
82	Provide an asset criticality score per device asset. Asset criticality indicates the importance of an asset in an organization. Administrators should be able to manually change asset criticality.		

RFP for Supply, Installation and Maintenance of
Cybersecurity Solutions and Associated
Hardware at the Bank

83	Provides insights into the organization's security posture using an Executive level dashboard. Must be able to show the company's overall risk score, individual asset risks, a view of ongoing attacks and their contributing risk factors.		
	Provides the ability to assess and mitigate vulnerabilities related to users, devices, and device assets on an Operations dashboard.		

Technical Specifications for Breach and Attack Simulation with Red Team Solution			
S No	Minimum Technical Specifications	Vendor's Compliance	Vendor's Remark
1	The proposed solution must be supported by an in-house and external threat intelligence group for providing threat updates on a regular basis, including features such as daily malware feeds and must also include attack Tactics, Techniques, and Procedures (TTPs) from multiple APT groups including those based on the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework		
2	The proposed solution should be able to simulate multiple attack vectors like:		
3	Network Infiltration Attacks		
4	End Point Attacks		
5	Email Infiltration Attacks		
6	Web Application Attacks		
7	Data Exfiltration Attacks		
8	Web Gateway and Proxy		
9	Threat Intelligence Exposure		
10	Full cyber kill chain attacks		
8	The solution must provide emerging threats without requiring additional licenses and the same should be included as part of the solution.		
9	The proposed solution must be deployed On-Premise i.e. at bank's DC and DRC. However the proposed solution should support Bank's infrastructure hosted on cloud		
10	The proposed solution must have the capability for on-premise installation of attackers, in order to allow for the simulation of attacks to originate on-premise instead of from the cloud, if needed by the customer		
11	The solution should include multiple On-Premise Attackers modules with the Complete Threat Library.		
12	Threats contained in the threat database of the proposed solution should be referenced according to the following set of information, including but not limited to:		
13	a) Unique identification number of the threat (unique ID),		
14	b) Release date of the threat,		
15	c) Text-based description of the threat,		
16	d) The severity of the threat is according to the following scale: Low, Medium, High.		
17	e) Affected Platforms,		

18	f) Targeted Sector,		
19	g) Targeted Region		
20	h) Attacker's Objectives, Actions		
21	i) Payloads, Executed Process Command Lines or Hash Values based on Attack Type		
22	j) References in publicly known databases like VirusTotal and other malware information sources		
23	k) References in the following industry-recognized threat scoring and enumeration systems: CVE, CWE, CVSS, OWASP		
24	l) Operating systems affected by the threat		
25	The OEM must add new globally critical attacks to the threat library within 24 hours, available for simulation.		
26	The solution should allow users to create new attacks by integrating samples from other platforms without OEM intervention.		
27	The proposed solution should be able to support browser agents for quick IPS/IDS/Web Gateway testing over https		
28	The proposed solution should be able to provide in-built Threat campaigns like Emerging threats, Top 10 ATT&CK techniques, Top 10 Ransomware attacks, Top Vulnerabilities exploited by State actors etc.		
29	The proposed solution should provide relevant payloads (availability of at least Hash Values, TTPs and RegEx provided by the BAS tool), signatures for the threats not available by default with Prevention technologies.		
30	The solution must continue simulations even if some techniques/actions are blocked, ensuring comprehensive results for all stages of the kill chain.		
31	The solution must provide detailed results with IoCs and pass/fail criteria for each kill-chain stage and continue evaluation even if some stages are blocked.		
32	The solution should provide real payloads and complete attack details, not just IoCs.		
33	In the proposed solution, the attack simulations must avoid trying to access real Command and Control (C2) URLs or any actions that could expose the network to actual malware or attackers		
34	The proposed solution should provide the result of every specific action of the threat actor individually. Result should specifically depict if action was blocked, not blocked and objectives of threat actors were achieved or not achieved		
35	The proposed solution should also provide details of the specific action that technology is not able to block while simulation		
36	The proposed solution should safely simulate attacks to get accurate map of the Security resiliency : The proposed solution's components should run attack simulations among its components and should not initiate connections to any production applications and endpoint systems to provide a risk-free assessment unless configured for lateral movement		
37	The proposed solution should be able to run multiple simulations in parallel with multiple agents		

38	The proposed solution must allow for the configuration of time delay between each action and protocol (HTTP/HTTPS) wherever applicable		
39	The proposed solution must not send Web Application Attacks targeted towards the customer's web applications to avoid any potential harm or performance instability. Instead, the proposed solution must send the web application attacks towards a component of the solution itself (like an agent)		
40	The proposed solution must not require specific response customizations for Web Application Firewall (WAF) assessment		
41	The proposed solution should use actual threat payload for security control assessment rather than using "PCAP playing" for web application attacks		
42	The proposed solution should also perform Web Application Attacks over both HTTP and HTTPS and should allow users to change HTTP and HTTPS default ports		
43	The proposed solution should also cover Data exfiltration techniques including HTTP, HTTPS & TCP protocols		
44	In the Data Exfiltration Assessment activity, the solution should send files in an encrypted format instead of clear text		
45	The proposed solution should be able to validate URL filtering capabilities against different URL categories		
46	The proposed solution should include URL categories within its database as templates		
47	The proposed solution should allow users to easily import custom URLs to be validated		
48	The proposed solution should allow users to configure the expected response while trying to access the URL as the result condition		
49	The proposed solution should imitate malicious methods used by APT's (Advanced Persistent Threats) while testing on Windows, Linux, MAC etc endpoint security controls, without infecting the underlying operating system.		
50	The proposed solution should have on-premises agent based/ agentless component of Breach Attack Simulation (BAS) which would be used to access the security posture of the target production environment (inside-to-outside, outside-to-inside, inside to-inside, and lateral movement), gain insights into the effectiveness of applicable security controls		
51	The proposed solution should support HTTP & HTTPS protocols for testing network security controls. All applicable Network Infiltration (file download) attacks should run over these protocols		
52	The proposed solution should validate the threat facing Cyber Security technology like Firewall, IDS/IPS, Antivirus, EDR, Web Application Firewalls, XDR & SIEM.		
53	The proposed solution should allow users to add Play and Rewind processes with at least the following information to be added:		
54	a) Path and Argument,		
55	b) Ability to Add a Remote File		

56	c) Ability to Use a Local File		
57	d) Define Result Logic		
58	e) Metadata Information		
59	f) Action Details		
60	The proposed solution should provide ready to use, user-customisable dynamic threat templates for Security Posture Management such as Readiness Against Ransomwares, Readiness Against APT Groups		
61	The proposed solution should be able to Create dynamic attack groups so that future attacks are automatically added into the group.		
62	The proposed solution should provide the custom creation of dynamic templates with filters such as Threat Name, Tags, Attack Category, Threat Actors, Unified Kill chain, MITRE ATT&CK Tactics, Affected OS, Severity, Release Date.		
63	The proposed solution should display the utilization and effectiveness level of a Cyber Security technology, expressed as a percentage, number of blocked and not blocked threats per simulation		
64	The proposed solution should provide access to MITRE ATT&CK framework coverage in the web interface for each simulation		
65	The proposed solution must provide a unified MITRE ATT&CK heatmap that integrates and shows prevention and detection scores of MITRE ATT&CK techniques		
66	The proposed solution should provide the custom creation of dynamic templates with filters such as Threat Name, Tags, Attack Category, Threat Actors, Unified Kill chain, MITRE ATT&CK Tactics, Affected OS, Severity, and Release Date.		
67	The proposed solution should allow users to upload their custom attacks, Malicious Codes or Vulnerability Exploits payloads, Hashes etc to the Threat Repository for web application attack, email attack, network infiltration attacks, End Point attacks and data exfiltration attack		
68	The proposed solution should allow for the creation of multiple and customizable profiles –		
69	a. admins,		
70	b. analysts and		
71	c. viewers with monitoring authorization levels only.		
72	Customizable options should be as follows: (a) Simulations (b) Templates (c) Agents (d) Custom Threats (e) Custom Actions (f) REST API Token (g) Organization Management (h) Mitigation		
73	The proposed solution must allow access through a web interface and RESTful APIs. The proposed solution should support integration and communicate with other solutions based on an “Application Control Interface” (API) access or the Syslog protocol, for purposes such as:		

73.1	(a) Customized reports		
73.2	(b) Customized dashboards		
73.3	(c) Integration with third party solutions like SOAR, SIEM or other platforms		
73.4	(d) Creating Dynamic & Static Templates		
73.5	(e) Creating Simulations & Re-run Simulations		
73.6	(f) Export Mitigations		
73.7	(g) Export Threat Lists		
74	The proposed solution should allow the status of "not blocked" threats and signatures to be exported via CSV format.		
75	The proposed solution should display the utilization and effectiveness level of a vendor technology, expressed as a percentage, number of blocked and not blocked threats per simulation for a number of supported technologies of leading vendors		
76	The proposed solution should support vendor-specific mitigations for globally leading vendors of Prevention & Detection Controls		
77	The proposed solution should uniquely identify and associate mitigation signatures of Cyber Security Technology with threat library content, by presenting a signature ID, Signature Version, Product version, Vendor assigned native Criticality associated with each threat in the threat library		
78	The proposed solution should provide relevant Payload , signatures for Threats not available by default with Prevention technologies like NGFW		
79	The proposed solution should present and classify signatures and mitigations by severity and category (web application attacks, vulnerability exploitation, malicious code) of the related threats for a number of supported technologies of leading vendors		
80	The proposed solution should allow signatures or threats to be searched and filtered using threat, action or signature names for a number of supported technologies of leading vendors		
81	The proposed solution should allow users to filter mitigation suggestions based on simulations and vendor type for a number of supported technologies of leading vendors		
82	The proposed solution should allow users to filter non-tempering Malware Engine signatures to be shown or hidden on demand for a number of supported technologies of leading vendors		
83	For security gaps revealed during the web application and network infiltration assessments, the proposed solution should provide vendor-specific mitigation suggestions on a dedicated dashboard on the interface for a number of supported technologies of leading vendors		

84	For security gaps revealed during the Windows Endpoint Scenario and Email assessments, the proposed solution should provide generic mitigation suggestions on a dedicated dashboard on the interface for a number of supported technologies of leading vendors		
85	The proposed solution shall allow using "vendor severity" to filter signatures to prioritize and start mitigation actions for a number of supported technologies of leading vendors		
86	The proposed solution should have the ability to analyse whether the threats in the tested attack vectors are detected and alerted on "Security Information and Event Management" (SIEM) and Endpoint Detection and Response (EDR) solutions by connecting to the relevant solution platform(s).		
87	When connecting to the SIEM, EDR and other such security solutions, the proposed solution must provide a connection via " API "using username-password authentication or token.		
88	The proposed solution should be able to provide Log Source Information to log necessary actions for the SIEM & EDR being used by the Bank		
89	The proposed solution should report the total number of simulated threats logged, not logged, or alerted, not alerted for each simulation		
90	The proposed solution will be able to show the "start time" of the simulated attack, "the end time", "the time between two periods" and in addition, the "logging time", "the time between the end of the attack and logging", "the time between the end of the attack and the occurrence of the alert"		
91	The proposed solution must provide an interface to add attack detection query time difference caused due to network delays or security vendor's time differences, by specifying an attack start early interval and an attack terminated delay interval.		
92	The proposed solution must provide an interface to limit the number of raw logs imported from SIEM to the management server to avoid high resource consumption on SIEM Solution		
93	The proposed solution must also provide an interface to define a limit on concurrent queries that can be made to the SIEM/EDR solution to perform detection analysis on parallel threats at the same time		
94	The proposed solution should give insights to get a holistic visibility of threat detection and response capabilities and accelerate the operationalization of the MITRE ATT&CK Framework		
95	The proposed solution should categorize the issues based on criticality:		
96	a. High - Rules that are malfunctioning or not functioning due to any issue		
97	b. Medium - Rules with optimization and performance issues		
98	c. Low - Rules with no issues and/or MITRE mapping		
99	The proposed solution should be able to move laterally to achieve a defined object by the admin, without using an agent, while evading its operations from security controls.		

100	The proposed solution should allow users to initiate the actions with various binary executables such as:		
101	a)Execution via New Threat Creation		
102	b) Execution via APC Injection,		
103	c)Execution via Call-Back		
104	The proposed solution should have the following attack methods in this module:		
105	a)Lateral Movement		
106	b)Kerberoasting		
107	c)Local Privilege Escalation		
108	d)Harvesting and Spreading Actions		
109	The proposed solution should have the following harvesting actions available:		
110	a) Local Service Misconfiguration Enumeration,		
111	b)Remote Management Users' Enumeration,		
112	c)Session Enumeration,		
113	d) LSASS Credential Dumping,		
114	e) Domain Object Enumeration,		
115	f)Domain DNS Enumeration,		
116	g) Organization Units Enumeration,		
117	h) Domain Trusts Enumeration,		
118	i)Domain Service Account Enumeration,		
119	j)Remote Desktop Users' Enumeration,		
120	k)Distributed COM Users Enumeration		
121	l)Local Admin Enumeration		
122	The proposed solution should have the following access actions available:		
123	a) Windows Management Instrumentation (WMI)		
124	(b) Server Message Block Execution (SMBExec)		
125	(c) Pass the Ticket (d) Bypass UAC via Fodhelper		
126	The proposed solution should have the capability to export lateral movement findings as a CSV report with following information:		
127	a) Discovered Hosts (IP and Name),		

128	b)Discovered AD Group DNS		
129	c) Discovered Domain Users (Username and Password)		
130	The proposed solution should map the lateral movement of the simulation in the GUI		
131	The proposed solution must help to understand if an attacker could obtain domain admin privileges by acquiring the highest level of access in the Bank's Active Directory Environment		
132	The proposed solution must be able to simulate ransomware behavior and help to understand which files the attacker can access and exfiltrate		
133	The proposed solution should report findings as a CSV report with following information: a) Discovered Hosts (IP and Name), b)Discovered AD Group DNS c) Discovered Domain Users (Username and Password)		
134	The proposed solution must support an AI smart assistant to help administrators do their operational tasks and provide users with insights to facilitate decision-making and optimize outcomes		
135	The platform must support to-the-point insights about security posture, most critical gaps and suggested mitigations and simple analysis of simulation results through the AI smart assistant		
136	The proposed solution must have the capability to integrate with Cyber Threat Intelligence		
137	The proposed solution must allow for filtering of Cyber Threat Intelligence data based on threat profile by Sector, Country, Region		
138	The proposed solution must support curation of organization-specific threat profile based on threat landscape and organizational context, such as industry, geography, asset landscape, etc		
139	The platform must support gen AI-driven collection, aggregation and curation of threat intelligence		
140	The platform must have the in-built capability to add attack detection query time difference caused due to network delays or security vendor's time differences, by specifying an attack start early interval and an attack terminated delay interval.		
141	The proposed solution should allow users to create custom dashboards for required simulations		
142	The proposed solution should allow users to compare their Prevention scores to industry, region, and platform averages		
143	The proposed solution must provide benchmarking of the Bank's security scores with average security scores of 10 for most simulated threats, threat templates, and ATT&CK tactics simulated by other customers		
144	The proposed solution must also offer threat landscape filtering by malware family and threat actors to allow for specific focus of attack simulation		
145	The proposed solution should allow administrators to access Audit Logs via Web UI and analyse with filtering options. The proposed solution should allow administrators to configure Syslog Integration to forward Audit Logs via		

	TCP or UDP to a log collector as CEF or JSON formats. The proposed solution should allow administrators to export Audit Logs via CSV file.		
146	The proposed solution must allow access through a web interface and RESTful APIs. The proposed solution should support integration and communicate with other solutions based on an "Application Control Interface" (API) access or the Syslog protocol, for purposes such as:		
147	a) Customized reports,		
148	b) Customized dashboards,		
149	c) Integration with third party solutions like SOAR, SIEM or other platforms,		
150	d) Creating Dynamic & Static Templates,		
151	e) Creating Simulations & Re-run Simulations,		
152	f) Export Mitigations,		
153	g) Export Threat Lists		
154	The proposed solution should be able to automatically schedule reports in PDF format on Weekly, Monthly basis for:		
155	a. Executive Summary Report		
156	b. Technical Report		
157	The proposed solution should provide trend of security posture over period of time		
158	The proposed solution should be able to notify users in Dashboard and via email.		
159	a) When a simulation agent is down,		
160	b) When an integration agent is down,		
161	c) When an integration is unhealthy,		
162	d) When the overall score falls below or rises above a custom set threshold or defaults score change updates compared to 7 days ago.		

Technical Specifications for Phishing Simulation			
S No	Minimum Technical Specifications	Vendor's Compliance	Vendor's Remark
1	The solution should be deployed on premise or on cloud. If cloud based, the CSP (Cloud service providers) must be CERT-in empaneled and must comply with international standards such as ISO 27001:2022.		
2	Offered solution should have atleast 200 variety of pre-loaded templates for phishing, ransomware, smishing and vishing with monthly updates		
3	The solution should have multiple campaigns capability of 5+ Cyber Awareness Simulation for identifying users prone to Email, Sms, Voice, (Email based) QR, (EmailBased) Ransomware, Email Attachment(HTML) and WhatsApp based Phishing attacks.		
4	The solution should be available on On - Premise Model from day 1		
5	There should have no limitation on number of cycles of carrying out simulation campaign on CBI users when the solution is operated by CBI during contract period.		
6	Bidder should have the capability of managed services as well(complete activity will be handled by the bidder with his own resources which includes running a simulation campaign, training users and conducting quiz on CBI users) per year whenever CBI asks for it during the contract period)		
A	Regarding Simulation of Phishing e-mails:		
7	Offered solution should have option to customize the email template or create a fresh template as per CBI requirement.		
8	Offered solution should have option to send emails to all tentative participants in a whole or send the email in groups. Solution should able to create various sender groups based on CBI requirements.		
9	Offered solution should have option to customize the landing page or create a fresh landing page corresponding to the Phishing email and as per Bank requirement.		
10	The provided solution should have option to customize in such a way so that the landing page can be accessed from Internet as per the requirement of Bank. All required services/solutions required to do the same is in Bidder's scope.		
11	Offered solution should provide the user-wise tracking of Email Delivery, phishing Link Clicked & Data Submission in phishing simulation.		
12	Offered solution should allow to put Fake CC (n number) in the phishing simulation emails. Support customization of Email ID of the sender for phishing campaigns		
13	Offered solution should be able to track email reply on phishing emails.		
14	Offered solution should have the capability to use HTTPS url for phishing purpose		

B	Regarding Simulation of Phishing over QR Code:		
15	QR Code Simulation - The solution should have option to simulate QR based phishing simulation where user receives an email with an embedded QR code which redirects to a landing page if the code is scanned.		
C	Regarding Simulation of Phishing over whatsapp:		
16	WhatsApp Simulation - The solution should have option to simulate whatsapp based phishing where the user receives a message on whatsapp with customizable text and a simulated phishing link where user submit their data.		
D	Regarding Simulation of Ransomware and Attachment e-mails:		
17	Offered solution should have option to customize the email template or create a fresh template as per CBI requirement		
18	For Ransomware simulation, the attachment should support .exe. Even though Logo of other formats can be used like .docx, .xlsx, .pptx, .pdf, .jpg, .png etc.		
19	In case of .exe as attachment, upon download of infected file, it should show some known file format (Like MS word, ppt, excel, PDF, image file etc). thumbnail in user' folder.		
20	Upon execution of infected file, users screens should freeze for a significant time with a customization message over the windows screen.		
21	Following the screen freeze with customized message, infected user should receive a intimation about the Cyber awareness exercise either as a Pop-up over the screen or as email to the respective user.		
22	Ransomware simulation should work on all the currently supported Window Operating system and later versions.		
23	In Attachment-based Phishing simulation, HTML file download should be supported.		
E	Regarding Simulation of Smishing:		
24	Over the same platform of Offered solution should have option to simulate Smishing where solution will initiate the SMS to the set of users (as per user list available) with customizable text and internet link corresponding to a webpage.		
25	Embedded link in the SMS should be accessible over the internet.		
26	Approving the text of SMS from the competent bodies of telecom office is in scope of CBI.		
27	Offered solution should have option to customize the landing page or create a fresh landing page corresponding to the Smishing and as per CBI requirement. Landing page to be accessed from Internet Only.		
F	Regarding Simulation of Vishing:		

28	Over the same platform of Offered solution should have option to simulate Vishing where solution will initiate the pre-recorded voice-calls to the set of users (as per user list available) and ask the corresponding users to submit the response through numeric input.		
G	Regarding Learning Awareness module for Users:		
29	Offered solution should have learning module for users, module shall consist of video tutorials, PDFs, Infographics tutorials and presentations followed by Quiz exercises.		
30	Consider specifying SCORM (Sharable Content Object Reference Model) version compatibility (e.g., SCORM 1.2, SCORM 2004) and/or support for xAPI (Tin Can API) for broader compatibility.		
31	The Solution should have infographics available in multiple language.		
32	The Solution should have 500+ content in total available in multiple categories such as Time saver, Posters, Wallpaper, Comic Stripes, Newsletter, Infographics etc.		
33	The solution should ensure that screen savers and wallpapers adhere to CBI's brand guidelines and are updated regularly with current security themes.		
34	The Solution should be capable of custom SMTP configuration for sending the training emails.		
35	The Solution should be capable of customizing the course completion certificate within the tool itself with logo and signature.		
36	The solution should be capable to auto-generate completion certificate (soft-copy) preferably digital signature options to the users who successfully complete the training exercise/quizzes.		
37	The solution should have option for adding the organization's own content and to conduct awareness sessions and quizzes.		
38	All the offered learning exercises should be playable over internet browser only (IE, Chrome, Mozilla etc)		
39	Offered solution should be capable to auto-generate completion certificate to the users who successfully completed the training exercise/quizzes		
40	Offered solution should be able send unlimited reminders and escalation to manager to the users for uncompleted trainings.		
41	The Offered solution should have SSO authentication available for smooth on boarding of users.		
42	The Offered solution should MFA available for Admin Log in.		
43	The Offered solution should have gamified assessment available such as word search for training purpose.		
44	The Offered solution should have leaderboard of users based on their performance in training and awareness.		
45	Bidder/OEM to ensure that the content for User training/learning module should be deployed over internet.		

46	The bidder must provide customization option in simulation email templates and landing page. The bidder to provide all necessary support to CBI for creating templates during the contract period.		
47	The Bidder/OEM must provide customised infographics as per Banks theme.		
48	The Bidder/OEM must conduct Quarterly Webinar Session for CBI employees for general security awareness.		
49	The Bidder/OEM must provide detailed customised video of campaign/ simulation ran at CBI at the end of campaign.		
50	Bidder/OEM to provide all Public URLs, Domain, sender email IDs etc resembling to the CBI domains required for simulating Phishing, Ransomware, Vishing, etc at no extra cost.		
51	Bidder/OEM to provide SMTP email Service/application for the simulating emails for the entire cyber awareness campaign. All the emails to be generated and deliver through that gateway only. If any public IP whitelisting is required to achieve the above, shall be enabled by CBI. SMTP solution/Application of CBI shall not be used.		
52	Bidder/OEM to ensure that the cloud services being used during the entire solution, should reside within India only.		
53	The Bidder/OEM has to conduct Quarterly Webinar Session for CBI employees for general security awareness		
54	The bidder/OEM must provide the reports generated during the cyber security simulation and awareness campaign (as per technical specifications).		
55	The bidder/OEM should provide Knowledge imparting sessions through User learning Portal.		
56	The solution should provide the Assessments and Quizzes to analyse the awareness levels of the employees after each awareness session.		
57	The bidder should provide one day tool training to Bank Team to use the tool by themselves, these users will also be provided with a Certificate.		
58	The bidder must sign Non-Disclosure Agreement (NDA) with CBI with a purpose of not sharing or using the data shared & collected during/from cyber security simulation and awareness campaign with anyone or anywhere.		
59	Complete implementation and commissioning shall be done within 30 working days from placement of Work Order/ LOA		
H	Phishing Incident Response- Reporting Button		
60	An email alert must be sent to the SOC team for threat reports, with a configurable threshold.		
61	The system should assign a spam score to reported emails; preferably the solution should detail the criteria and methods used for assigning spam scores, including thresholds and algorithms, to ensure consistent and accurate threat assessment.		
62	The solution must scan the content of emails for threats and should verify SPF, DKIM, and DMARC to ensure emails pass these checks.		

63	The solution should verify SPF, DKIM, and DMARC email authentication methods to ensure emails pass these email authentication checks.		
64	Real-time database updates must be supported and Users should be able to see the threat percentage of the email.		
65	The system must allow users to download raw headers of emails and IP reputation checks should be performed.		
66	The solution should reputation of the sender's domain must be checked and Advanced protection for attachments and URLs/links is required.		
67	Include specific requirements for hash algorithm standards (e.g., SHA-256) and detail 2FA methods (e.g., OTP, TOTP) to ensure compatibility and robustness.		
68	The solution should perform deceptive domain checks and Users should receive notifications for reported, approved, or declined emails.		
69	The Solution must support multiple anti-virus scanning engines and DNS blackhole lists should be used for additional threat intelligence.		
70	The solution should perform deceptive domain checks and Users should receive notifications for reported, approved, or declined emails.		
71	The solution should provide header analysis capabilities.		

Technical Specifications for **Active Directory Security**

S No	Minimum Technical Specifications	Vendor's Compliance	Vendor's Remark
A	User Behavior Analytics		
1	The solution must be capable of sending behavior alerts via email to ensure timely notification based on identified threat patterns.		
2	The solution should support sending behavior alerts via syslog to enable integration with diverse logging and monitoring systems.		
3	The solution must have the capability to send behavior alerts via SNMP or alternative methods for direct integration with existing network management and monitoring tools.		
4	The solution should offer a mechanism to automatically trigger predefined actions in response to detected behavioral alerts, ensuring swift and proactive threat response.		
5	It must automatically identify, categorize, and alert on abnormal behavior related to administrator accounts, including both a typical and high-risk patterns in their activities.		
6	The solution needs to autonomously detect and flag behavioral anomalies associated with service accounts to provide early warnings of potential security risks.		
7	It must automatically recognize and alert concerning any unusual behavior from executive-level user accounts, enabling proactive measures against security threats.		
8	The solution should automatically identify behavioral patterns associated with executive data, generating alerts when abnormal activities are detected.		
9	It must employ behavior analytics to recognize and indicate patterns that correspond to known cyber threats and attack methodologies, raising alerts accordingly.		
10	The solution should use behavior analytics to detect abnormal user file access and issue alerts when suspicious patterns are identified.		
11	It must provide behavior analytics-based alerting for abnormal user folder access to indicate potential security breaches or unauthorized activities.		

12	The solution should offer behavior analytics-based alerting on abnormal user mailbox access to pre-emptively notify about potential security threats.		
13	It should use behavior analytics to alert on abnormal user device logons, signaling potential security issues or compromised devices.		
14	The solution should generate alerts when administrators exhibit behavior outside their standard activity patterns.		
15	It must generate alerts when abnormal behavior from service accounts is detected, indicating potential security vulnerabilities.		
16	The solution needs to alert when unusual or suspicious behavior is detected from executive-level accounts, enabling swift threat mitigation.		
17	It must provide alerts when abnormal access to executive data is detected, indicating potential breaches or unauthorized access.		
18	The solution should generate alerts for abnormal access to executive mailboxes to prevent data breaches or unauthorized access to sensitive information.		
19	It should generate alerts when it detects the presence of exploitation or reconnaissance tools in the system.		
20	The solution must alert administrators when abnormal activities within Active Directory are detected, indicating potential security breaches or attacks.		
21	It must alert when abnormal access to sensitive data is detected, preemptively indicating potential security threats.		
22	The solution should generate alerts for abnormal access to stale data, indicating potential security threats or breaches.		
23	It must provide alerts for activity indicative of ransomware, signaling potential security risks.		
24	The solution should alert when account passwords are reset, possibly signaling security concerns or unauthorized access.		
B	Alerting		
25	The solution should alert on permission change events with detailed context, including the nature of the change and affected resources, to provide comprehensive notifications.		

26	The solution must be capable of setting thresholds to trigger alerts on permission change events, allowing for a nuanced response based on the frequency or scope of alterations.		
27	It should alert on directory service events, signaling when changes or activities occur within the directory service environment.		
28	The solution must alert on group membership changes, providing notifications when alterations to user group memberships are detected.		
29	It should alert on changes to global security groups, signaling modifications to high-level security group structures within the organization.		
30	The solution should alert on GPO (Group Policy Object) changes, providing notifications for any adjustments made to GPO settings.		
31	It must be capable of alerting on events by user, offering insights and notifications specific to individual user activities.		
32	The solution should alert on events by container, providing notifications regarding changes or activities within specific organizational containers or structures.		
33	It must alert when critical Organizational Units (OUs) are modified, signaling potential structural or security changes within the organizational framework.		
34	The solution should alert when group membership changes for security accounts occur, ensuring timely notifications for crucial security-related alterations.		
35	The solution should be capable of generating alerts for complex threat models, identifying and signaling a wide range of sophisticated potential cyber threats and attack patterns.		
36	The solution must alert upon the identification of potential cyber threats and common attack patterns, providing proactive warnings based on recognized threat models.		
C	Permissions, AD, and Data Cleanup		
37	The solution must be capable of generating actionable reports on unused or empty security groups, including recommendations for remediation.		
38	It should provide reports on unresolved SIDs on ACLs (Access Control Lists) and Individual User ACEs on ACLs, highlighting any security identifiers or access control entries that lack clear identification.		

39	The solution should provide reports on inactive data and inactive users, identifying and reporting on data and users that exhibit prolonged periods of inactivity.		
40	It must offer a report detailing disabled users who remain in security groups, highlighting instances where deactivated users are still part of security configurations.		
41	The solution should have the ability to move or migrate unused data to a lower tier repository, facilitating the relocation of data that has shown a lack of recent activity to a secondary storage location.		
D	Misconfiguration Management		
42	The solution should help discover, document, and rectify Active Directory (AD) misconfigurations, offering detailed insights and automated remediation solutions for configuration issues.		
43	The solution must showcase findings on expired passwords, users with blank passwords and users with no password expiry.		
E	Activity monitoring and threat detection		
44	It should have the capability to detect and promptly alert on any abnormal activities, signaling potential security threats within the system.		
45	The solution should detect identity-based risks and threats like privilege escalation, providing crucial insights into potential breaches and vulnerabilities.		
46	It must effectively identify and alert about potential threats to the system, covering a spectrum of risks, including misconfigurations, external threats, and insider threats.		
47	It should not only detect risks but also provide comprehensive recommendations to mitigate these identified risks, offering actionable strategies for security enhancement.		
48	The solution must offer in-depth insight into various attack methods and provide actionable intelligence on tactics and procedures used by potential threats, including mitigation strategies.		
49	The solution should not only map alerts to MITRE ATT&CK tactics and techniques but also provide a user-friendly interface for understanding and contextualizing threats and attack methodologies.		
50	The solution should identify and analyze patterns of failed user authentication attempts from a single device or IP, including distinguishing between password guessing and other attack vectors.		

51	The solution must detect and prevent attackers from utilizing elevated privileges to compromise computers in the domain, including domain controllers.		
52	The solution should identify potential Kerberoasting attacks, wherein attackers attempt to harvest tickets with low encryption to crack passwords.		
53	The solution should detect and respond to abnormal login attempt patterns indicative of potential attacks, such as repeated login attempts from multiple devices, indicative of username guessing or credential stuffing. It should also identify and differentiate between credential stuffing attacks, brute-force attacks, and their subsequent phases, alerting and potentially triggering countermeasures upon detecting suspicious activities, such as rapid and persistent username and password guessing attempts.		
54	The solution must be capable of detecting gradual brute-force attacks, aiming to compromise multiple admin credentials or cause denial-of-service for multiple admins. The system should promptly alert and respond to such threats to ensure proactive security measures.		
55	The solution should detect a potential brute-force attack intended to steal various admins' credentials or cause denial-of-service for multiple admins.		
56	The solution should detect and flag potential attempts by an attacker to install malicious services for persistency and as part of lateral movement. Unusual activities, especially those not previously observed for the user in question, should be identified and flagged promptly.		
57	The solution must detect a gradual brute-force attack aiming to steal various users' credentials or cause denial-of-service for multiple users.		
58	The solution should indicate a gradual brute-force attack targeting a user's credentials or denying user access.		
59	The solution must flag accounts without behavioral profiles, indicating an attacker's gradual search for their target data within the network.		
60	The solution must be able to identify potential gradual brute-force attacks targeting the admin's credentials or attempting to deny admin access. The system should provide alerts and responses to mitigate such threats promptly.		

61	Custom alerts must be highly configurable, allowing users to set detailed criteria, thresholds, and escalation procedures based on their specific security requirements		
62	The solution's threat models must be regularly updated, ensuring that the system is fortified against the latest threats and vulnerabilities.		
63	Alerts generated by the solution should be directly sent to the relevant personnel, ensuring swift response and action against any potential security threats.		
64	The AD Security Solution should integrate seamlessly with a range of SIEM and other security solutions to provide comprehensive security monitoring and management.		
65	It should use both Syslog and/or APIs to feed logs to SIEM solutions and other such security solutions, allowing for versatile and multi-platform log sharing.		
66	The process for exporting audit logs should be straightforward, allowing users to access and export logs efficiently and conveniently.		
67	The solution should offer either an incident response team or services, assisting users in effectively addressing security incidents.		
68	It should provide forensics services, enabling users to delve deeper into security incidents for thorough investigation and analysis.		
69	The solution must integrate with SOAR (Security Orchestration, Automation, and Response) platforms and provide seamless interoperability with existing security tools to streamline incident response and security protocols.		
70	The solution must secure Microsoft Active Directory which is currently running on Windows 2016 Server and must support higher version of Microsoft Operating system e.g. 2019, 2022 and on later versions		
71	The Bank Active directory consist of about 42000 Computer Systems etc.		
72	Solution should discover the AD structure and permissions, including user objects, groups, computers, OUs, etc.		
73	The Solution should be able to streamline user and group administration through provisioning & de provisioning, solve security issues – and meet those never-ending compliance requirements by managing and securing on-premise AD simply and efficiently with a single, intuitive solution.		
74	Solution can audit GPO changes and detect unauthorized activity in AD		

75	The Solution must be able to audit GPO changes.		
76	The Solution should be able to track changes in AD like User creation /deletion /modification, Groups, group policies, DNS. Provide alerting and reporting for the critical changes. Capability to provide all regulatory compliance reports like PCI etc.		
77	The Solution should be able to provide deep visibility into Active Directory (AD) users, groups, roles, organizational units and permissions by providing detailed reports on various aspects of it. Apart from reports, it should also perform security assessments, configuration change history reviews etc.		
78	The solution should be able to provide a central report of implementation of a Group Policy success / failure Report of Systems/ Users .		
79	The Solution should be able to provide DNS Security.		
80	The Solution should be able to provide central report for logging activity of users and computers. If the solution requires agent then it should be provided.		
81	Solution should have the capability to alert if an unauthorized attempt is made for configuration changes in AD		
82	Solution should have real-time tracking, analysis and reporting on all Microsoft Active Directory events.		
83	Solution should have real-time tracking, analysis and reporting on all Microsoft Active Directory based and LDAP queries		
84	Web-based access with dashboard reporting.		
85	Solution should have capability to Identify queries against Active Directory (AD) that are not secure or signed.		
86	The Solution should be able to effectively administer and control Group Policy Object (GPO) changes and verify, compare, update and roll back GPO versions. Ability to confirm the consistency of various GPO settings.		
87	The Solution should be able to streamline user and group administration through provisioning & deprovisioning, solve security issues – and meet those never-ending compliance requirements by managing and securing on-premise AD simply and efficiently with a single, intuitive solution.		
88	The Solution should provide Reviewer-Approver facility for Role based access and Real time notifications for the administrative activities.		

89	The Solution should be able to streamline user and group administration through provisioning & de-provisioning, solve security issues – and meet those never-ending compliance requirements by managing and securing on-premise AD simply and efficiently with a single, intuitive solution.		
90	The solution should have a capability to generate comprehensive change reports from compliance purpose.		
91	Proposed third party system should proactive, approach to AD Management. Complete GUI feature for user management, user life cycle, privilege allocation and revoke, various report for top management such as users under OU, transfer of users from OU to other, user revoke or disable, number of users logged in in real time basis, number of users successfully logged in for last day, last 7 days, last month etc. with complete details of user such as employee id, name, designation etc. Extraction of report in pdf, excel and machine printable format.		
92	Proposed solution should proactive, risk-based approach to AD security, users can all the associated vulnerabilities, predict which pathways attackers may target, and act to detect, shut down and prevent attacks.		
93	The solution should have Review-Approve facility for all admin activities. Privileged access for Users.		
94	Solution should be able to Disable the accounts automatically on expiry of validity period.		
95	Solution should be able to Facilitates notification to concerned users on completion of the execution of a task.		
96	Solution should be able to Automatically lockdown privileged accounts that are inactive for a period of time.		
97	Proposed solution should throw warning message and reports for abnormal activities like password reset of around 50 users of one Region, password reset of one user twice a day, User creation with identical name, user movement from one OU to other twice a day, any activity done beyond normal working hours (i.e, other than 10:00 AM to 06:00 PM)		
98	Proposed solution should capture IP address of the system while logging-in to the solution or while initiating any request through the solution, which may not require to log-in to the solution		

Technical Specifications for Governance, Risk and Compliance			
S No	Minimum Technical Specifications	Vendor's Compliance	Vendor's Remark
A	Business Impact Analysis:		
1	The system must facilitate the comprehensive assessment of business processes to determine their criticality and the impact of disruptions.		
2	Templates should be provided for conducting BIAs and customizable fields for different types of impact (financial, operational, legal, etc.).		
3	The system must allow for the estimation of Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objectives (RTO), and Recovery Point Objectives (RPO) for each business process.		
4	It should enable the identification and documentation of interdependencies between business processes, applications, vendors, locations, employees and skills, and other related processes.		
5	The solution must have the capability to store and update the Recovery Point Objectives (RPO) for data and system restoration.		
6	The system must catalogue all resources required for recovery and continued operations, including human resources, technology, information, facilities, and financial considerations.		
7	The system should enable users to specify alternate resources and workarounds for each critical process, should primary resources become unavailable.		
8	The system must provide the capability to attach or store documentation related to the Business Impact Analysis.		
9	The system should provide configurable approval/review process on BIAs. It should also allow reminders, escalation, overdue notification for the BIA's to be responded to in a timely manner.		
10	The system should allow the storage of historical BIA's against any of the processes.		
B	Business Continuity Plans:		
11	The system must support the creation and maintenance of comprehensive business continuity plans for each critical business function.		
12	The system must support the ability to create detailed Disaster Recovery Plans (DRP's) which may be linked to IT services/applications.		
13	The system should offer step-by-step guidance for response and recovery activities, including predefined tasks, responsible parties, and communication strategies.		
14	The solution must allow for the attachment of relevant documents, such as site plans, contact lists, and resource requirements.		

15	The system should enable the linking of BCPs to corresponding Business Processes and Org Hierarchy.		
16	The system must facilitate the definition and documentation of roles, responsibilities, and escalation protocols for all staff involved in business continuity, ensuring clarity and swift decision-making during a disruption.		
17	The system should allow the user to define initial response activities.		
18	The system must allow users to specify which business processes, applications, and vendors are covered by each BCP.		
19	The solution should include templates and tools for developing comprehensive communication plans, addressing both internal and external communications.		
20	The system must provide features to document recovery sites and alternate work locations		
21	The solution should outline detailed recovery steps for resuming business operations, including prioritized actions, timelines, responsibility and other details.		
22	The system should have the capability to define multiple templates for various BCP categories.		
23	The solution must allow the configuration of a flexible workflow for BC Plan review and approval.		
24	The solution must have the capability to remind the review of all BC Plans based on the frequency set in the plan itself		
25	The system should allow a capability to invoke a BC Plan in case of a Crisis. It should allow the capability to invoke a BC Plan and the workflow for an activated plan should be triggered and relevant notifications should be sent out.		
C	Exercises:		
26	The system should have functionality to plan, schedule, and document business continuity exercises.		
27	The system should offer customizable templates for various types of exercises, including integration with external simulation tools, for tabletop exercises, walkthroughs, simulations, and full-scale drills.		
28	The system must allow for the specification and documentation of roles and responsibilities for all participants in the exercise, ensuring clarity of action and accountability.		
29	The system should provide the capability to associate each exercise with relevant Business Continuity Plans (BCPs).		
30	The system must include features to manage and document vendor participation, including expected contributions to the exercise.		
31	The solution should allow for the creation and documentation of exercise scenarios, defining the objectives, scope, and expected outcomes.		
32	The system must provide tools for pre-exercise impact assessment to predict potential outcomes and prepare for real-life business disruptions.		
33	The system should include functionality to create a timeline for each scenario, outlining the sequence of events and anticipated decision points.		

34	The system must track and record actions taken during the exercise, ensuring that each step is documented for later review.		
35	The solution should facilitate the capture and management of feedback and evaluations post-exercise, highlighting areas for improvement.		
36	The system must allow for the setting and assessment of success criteria to evaluate the effectiveness of the exercise and the readiness of the BCPs.		
37	The system must allow for recording of exercise outcomes, identifying gaps in plans, recovery activities and tracking improvement actions.		
38	The system should the allow the ability to draft action plans to fix the gaps identified as a part of the exercise.		
39	The solution must allow the configuration of a flexible workflow for the Exercise review and approval		
40	The system should include features that enables comprehensive recording of all details related to crisis events, encompassing the description of the event, recovery steps taken, subsequent improvement actions, and lessons learned.		
D	BCM Reporting:		
41	In view if the regulatory expectations, as a mandatory requirement for bank, the system should generate BCM reporting in various formats including MS Word, PowerPoint, Excel, and PDF with necessary branding as per Bank's expectation.		
Incident Management			
E	Dynamic Incident Submission:		
1	The system must offer a dynamic incident reporting form with a variety of configurable fields including text, numerical, date/time, dropdowns, checkboxes, radio buttons, lookup fields, and rich text for detailed descriptions.		
2	The system should adapt incident reporting forms based on user-selected categories to present only the relevant fields, streamlining the submission process.		
3	The system must allow conditional visibility of form fields, tailored by input in preceding fields to ensure form relevance.		
4	Each form field should provide descriptive tooltips, offering immediate, context-specific guidance.		
5	Users should be able to select from pre-defined incident reporting templates for consistency in data collection.		
F	Adaptive Workflows:		
6	Incident categories must determine the management workflow, routing incidents to the correct resolution paths and teams.		
7	The system must adapt workflow management based on incident attributes such as criticality.		

G	Incident Lifecycle Management:		
8	The system must capture extensive details for each incident, including category, main category, location, department, related assets, financial implications, and any other customizable fields deemed necessary.		
9	Incident assignments should detail the reporting individual/team and method of reporting.		
10	Notification settings must enable specific individuals to be alerted about the incident.		
11	The system must allow status and prioritization settings, including a color-coded priority level.		
12	A feature should exist to list affected assets and attach relevant documents.		
13	Users must be able to conduct thorough impact analyses and record multiple financial impacts.		
14	General comments related to the incident should be enabled.		
15	The system must provide a chronological tracking feature with real-time updates that visualizes the entire lifecycle of an incident from reporting to resolution and closure, including timestamps for key events.		
16	Assignment management within the system should include automated routing of incidents to appropriate individuals or teams based on predefined rules or manual selection.		
17	Customizable notification mechanisms should be provided to inform designated stakeholders about new and updated incidents, with settings for different channels and urgency levels.		
18	Integration with a knowledge base should be provided, allowing for quick reference to articles that can aid in the resolution of incidents, with automatic suggestions based on the incident's attributes.		
19	Task management for incident resolution must be robust, allowing for the creation of tasks, assignment to team members, tracking of progress, and linking to specific workflow steps.		
20	Documentation of lessons learned and improvement actions should be a feature of the system, with these learnings being accessible for future incident prevention and response planning.		
H	Knowledge Base:		
21	The system must facilitate the management of knowledge base articles with advanced search and filter functions.		
22	Detailed article structure including authorship, and attachments should be enabled.		
23	The system must feature a centralized repository for knowledge base articles that provides personalized article recommendations based on user queries and incident attributes.		
24	It should offer robust article management capabilities, including the ability to add, edit, archive, and delete articles through a user-friendly interface.		
25	Advanced search capabilities are required, including full-text search, keyword matching, and filtering by category, author, or related incidents, to quickly locate relevant articles.		

26	The system must support detailed article structures, capturing information such as title, summary, detailed content, related articles or incidents, and other metadata.		
27	The ability to attach supplementary files to articles, such as images, videos or documents, should be available, with support for common file formats.		
28	User interaction features must be provided, such as the ability to comment on articles, and suggest edits to foster a collaborative and interactive knowledge base.		
29	Integration with the incident submission process is required so that users can be prompted to consult the knowledge base before submitting an incident, potentially reducing unnecessary incident submissions.		
30	The system should offer a streamlined article submission and approval workflow, enabling contributions from various teams and departments and ensuring content accuracy and relevancy through a formal review process.		
I	Incidents Self-Service:		
31	The system must provide users with a self-service portal to track the status and details of incidents they have reported, with updates on progress and resolution.		
32	It should offer a resolved incidents archive where users can review past incidents they have reported along with the resolutions provided, fostering transparency and learning.		
33	Quick access to the knowledge base must be provided, enabling users to find solutions and information without needing to escalate to support teams.		
J	General Requirements:		
34	The system should support the creation of fully configurable and tailored incident management dashboards based on organizational needs.		
35	In view of the regulatory expectations, as a mandatory requirement for bank, the system should be able to support configurable report formats such as Word, PowerPoint, Excel, and PDF.		
36	The system should support an automated incident assignment based on predefined rules.		
37	Configurable incident escalation and notification settings should be available.		
38	Customizable incident workflows with defined stages and actions should be supported.		
39	Configurable incident details pages must be offered to suit organizational requirements.		
Information Security - ISMS - ISO27001:2022			
K	Policy Management:		
1	The system must enable the creation, review, and management of security policies with version control and audit trails.		

2	The system should offer the capability to either create policies directly within the system using a comprehensive set of tools and a rich text editor, or upload existing policies as documents.		
3	The system should notify relevant stakeholders of upcoming policy reviews and policy approval during creation.		
4	The system should have the capability to link policies directly to specific ISO 27001 Controls and Clauses and other relevant standards.		
5	The system should enables linking of related policies.		
6	The system should have fully configurable fields management to capture comprehensive policy details including policy ID, title, related Annex A controls, version, owner, effective date, review dates, review frequency, and other adaptable fields as needed.		
7	The system should allow attaching documents that are related to the policy for reference and compliance.		
8	The system should enable the tracking and management of the approval workflow and notification for each policy.		
9	The system must generate finalized policy documents, supporting both Word and PDF formats.		
10	The system must include configurable lookup fields for various regulations and additional controls that can be easily linked to relevant policies, supporting dynamic updates to the regulatory landscape.		
11	The system should offer the feature to link policies to a variety of standards beyond ISO 27001, allowing the organization to comply with multiple frameworks and enhance its compliance adaptability.		
L	Risk Assessment:		
12	The system must include a risk register with key details for each risk. The risk register table should allow for adding risk, filtering, searching, and inline editing of risk entries.		
13	The system must accommodate both asset-based and scenario-based risk assessments.		
14	The system should have the flexibility to add fields as required with support for dropdowns, checkboxes, and other form elements.		
15	The system should feature customizable risk forms with the option to create and utilize multiple form templates. Users can select from these templates, each offering different levels of detailed risk assessment features and processes.		
16	The system should have capabilities for documenting existing controls per risk, offering options to add controls, and defining their owners and types. Additionally, the system should facilitate linking these documented controls to the 93 controls specified in ISO 27001 Annex A.		
17	%The system should have options for risk treatment including mitigate, transfer, avoid, and accept, with the ability to add justification for chosen treatment option.		

18	The system should enable documenting risk consequences and causes, providing a comprehensive understanding of each risk.		
19	The system should feature heat maps for both aggregated and risk level that visually represents both inherent and residual risk levels.		
20	The system should have tools to list and add risk treatment plans, detailing treatment activities, linkage to ISO 27001 Annex A controls, assigned owner, start/end dates, and tracking of progress and budget.		
21	The system should enable the evaluation of residual risk likelihood and impact, with options to record justifications for each assessment.		
22	Ability to generate comprehensive risk level report capturing all risk details, including an overview, inherent and residual information, heat map, existing controls, treatment details, and risk analysis.		
23	Ability to generate Risk register reports in PDF, Word and Excel.		
24	The system should be configurable to support a risk workflow and approval process.		
M	Statement of Applicability:		
25	The system must assist in creating and maintaining the Statement of Applicability (SoA).		
26	The system should reflect updates to controls or risk status automatically in the SoA.		
27	The system should track and report on the implementation status of each control.		
28	The system should provide detailed controls pages that include information such as a Control Card (featuring Control Name, Applicability, Control Category, Description, Justification for Inclusion/Exclusion, and Status), Control Treatments (detailing Treatment, Owner, Start and End Dates, Progress, Status, Associated Risk, and Budget), as well as lists of Related Policies, Existing Controls, Control Documents, Findings, Related Audits, and an area for Control Comments.		
29	The system must have the capability to generate a Statement of Applicability (SoA) report in both PDF and Word formats, detailing all controls along with their applicability, justification, and status.		
N	Information Security Objectives:		
30	The system must help in setting, monitoring, and reviewing security objectives.		
31	The system should provide tools for measuring and reporting performance against objectives.		
32	The system must ensure that security objectives are aligned with overall business goals and can be reviewed periodically.		
33	The system should list the objective associated risks and treatment activities.		
34	Each objective must feature a risk heat map plotting all associated risks.		
35	the objectives should be linked to specific KPIs for measurement and associated initiatives to achieve them.		

O	Internal Audit:		
36	The system must have functionalities for planning and conducting information security audit programs where each program can include multiple audits.		
37	The system must have functionalities for planning and conducting information security internal audits.		
38	The system must integrate internal audit with ISO 27001 Clauses and Annex A controls.		
39	The system should manage and track audit findings and related corrective activities. The system should provide functionality to attach relevant working papers.		
40	The system should facilitate the definition of Audit Criteria for information security, including ISO 27001 Clauses, Annex A Controls, Standards, Policies, Compliance & Regulations, and allow for the inclusion of Other Criteria through a free text option.		
41	The system should feature detailed pages for each audit finding with interactive dashboards for tracking findings, criteria, and evidence.		
42	The system should provide aggregated dashboard and listing for managing and viewing non-conformities and corrective actions.		
P	Management Reviews:		
43	The system must support the scheduling and conducting of management reviews.		
44	The system should facilitate tracking of review action items.		
45	The system integrates inputs from various sources (like audits, incidents, and performance metrics) for comprehensive review.		
46	The system allows for the customization of review templates and processes to fit organizational needs.		
47	For each management review, the system must capture comprehensive details including feedback, action items, and progress tracking.		
Compliance Management			
1	The solution must allow the capability to maintain a Compliance Library with multi-level categorization and tagging of regulations.		
2	The solution must allow the mapping between the regulation and the controls (to be stored in a control library).		
3	The system should have the ability to define control characteristics, such as type, significance, and frequency of testing etc		
4	The system should have a comprehensive search capability across the Compliance Library.		
5	The solution should support the ability to define, document, map, monitor, test, assess, and report on controls within the control library.		

6	The solution must have the ability to scope and schedule the control testing. Allow different types of testing such as design testing, operating effectiveness testing and control self-assessments.		
7	The solution must allow the mapping of controls in the library to various different entities within the system such as regulations, policies, assets etc.		
8	The solution should provide a complete overview of your company's compliance in a single view.		
9	The solution must allow the configuration of a flexible workflow for the control scoping, scheduling, testing, reviewing, reminders, escalation and action plan tracking		
10	The system should highlight and track open issues against weak control effectiveness ratings, enabling action plan creation and prioritization.		
11	The solution must be able to track the progress update of the action plans and send reminders/escalations if required.		
12	The solution must allow the reassignment of Action Plans.		
13	The solution must allow the prioritization of the action plans based on importance.		
14	The solution must provide the capability to enable a workflow on action plans for timely monitoring and validation.		
15	The system must have the ability to distribute assessments to multiple groups or individuals.		
16	The solution should support a risk-based approach to compliance and the sharing/reuse of control measures between compliance and risk.		
17	The solution must support the ability to monitor, document, and manage changes to the regulatory environment with historical tracking.		
18	The solution shall have the ability for management to identify and document key controls in relation to compliance obligations/risks.		
19	The solution should be configured to have a compliance register with definable fields.		
20	The solution can manage non-compliance incident impacts, ratings, and metrics.		
21	The solution should provide proactive monitoring, including status tracking, automated reminders, and progress updates.		
22	The solution should notify users when tasks need to be performed.		
23	The solution has ability to document, update and track corporate compliance obligations landscape.		
24	The solution should be able to generate compliance reports and dashboards in a variety of formats including PDF, Word, and PPT.		
25	The solution should provide an organisation-wide view of the compliance universe.		

26	The solution should support compliance for regulatory and organizational compliance frameworks.		
27	The solution should support standard and custom processes related to the different laws/regulations/best-practices.		
28	The solution must have the capability to add comments and attachments to any page, with version control for attachments.		
29	The system should be equipped to send notifications based on predefined business rules.		
30	The system must include sophisticated filtering options for data within tables, enabling users to sort and access specific information based on column content.		
31	In view of regulatory expectations, the system should support the generation of risk and compliance reports in various formats.		
IT Audit			
Q	Planning & Universe:		
1	The solution must have the capability to prepare Audit Plans over any time horizon, be it 3 months, 6 months, 12 months or 3 years.		
2	The solution must manage Audit cycles including (audit planning, resource scheduling/calendaring, work paper management, and audit Issues. Follow up management).		
3	The system has the ability to maintain a comprehensive Audit universe encompass all business units, processes, systems, associated risks of the organization etc.		
4	The solution must include advanced analytics to assess and prioritize audit areas based on evolving risk metrics and historical data trends.		
5	The solution must have the capability to capture budget/plan time for each audit engagement at the time of planning. The system allows for start and stop dates and other milestones of an audit to be planned and tracked for all metrics, including Planned, revised planned and actual dates, kick-off date, draft report date, closing meeting date, audit close date, etc.		
6	The solution must be able to automatically calculate the next date an audit assignment for when it should next be performed based upon designated criteria		
7	The solution must have the capability to automatically create individual audit plan directly from the Annual Audit plan on a web-based mode.		
8	Need to have a robust process for approval of the annual internal audit plan with segregation of duties in effect.		
10	The system allows for confidential audits for fraud, or other related internal reviews, to be scheduled but hidden from views and auditors without access to them.		

R	Resource Allocation and Audit Program:		
11	<p>The system allows for creating a key team to do necessary planning checklists to ensure audit steps comply with internal procedures and ensure work papers and documentation for each step to be easily assessable from the checklist.</p> <p>The solution must have the capability to alert the supervisor while planning the resources, if the auditor is already assigned to another project.</p>		
12	<p>The solution must have the capability to Track Actual Time spent in each phase of the audit that allows for reporting of specific audits performed by individual auditors, teams etc</p> <p>The system allows for time budgets to be created for each audit and audit section, Time sheets to be filled out where it compares actual time vs. budget time by audit, by year, etc., and allows for time sheets to be reviewed and approved.</p> <p>The solution must have the capability to approve auditors' hours online.</p> <p>The system allows for start and stop dates and other milestones of an audit to be planned and tracked for all metrics, including Planned, revised planned and actual dates, kick-off date, draft report date, closing meeting date, audit close date, etc.</p>		
13	The solution must have the capability to capture planned time for each audit staff.		
14	The solution must have the capability to report audit vs. non-audit time, and comparison to budgeted time.		
15	The solution must have the capability to generate administrative reports by auditor and audit assignment.		
16	The solution must have the capability to prohibit/ restrict time entries after specific audit project closeout.		
17	The system must allow the ability to scope the entities from the audit universe which are in scope for the current audit		
18	<p>The solution must have the capability to access the audit procedures captured in the audit program to conduct the audit.</p> <p>The solution must have the capability to add additional audit steps (procedures) to the audit program at any time during the course of the audit.</p>		
19	The solution must have the capability to enable the audit supervisors to approve the audit program and any subsequent changes.		

20	The solution must have the capability to send and file the letter of introduction/notification to auditees for audit commencement.		
21	The solution must have the capability to store and retrieve audit programs, templates and repetitive issues in a repository		
S	Workpapers:		
22	The system allows for audit work papers to be created directly from an audit program and automatically referenced back and allows for multiple types of work papers to be created, including templates for interviews, meetings, or control tests.		
23	The system must allow for more than one audit issue to be generated per work paper, and can be attached directly to work papers, automatically referenced, assigned expected completion dates, issue coordinators, priorities, and assigned dispositions such as audit report or verbal discussion.		
24	The solution must have the capability to assign risk severity levels to each Audit Issue		
25	The solution must have the capability to capture audit conclusions and recommendations.		
26	The solution must have the capability to record multiple recommendations for each audit and issue		
27	The status of audit issues as per published internal audit reports should be able to be seen through the use of dashboards (i.e. open/closed/late/agree/disagree) etc.		
28	Generate audit reports based on user requirements (e.g. task status/audit notes etc.)		
29	Ability to perform quality assurance on audit tasks and or the audit file prior to closure.		
30	The solution must have the capability to link or embed into the software any externally generated documents.		
31	The solution must have the ability to applying standard tick marks to working papers and scanned documents and these tick marks should be customizable to suite the office agreed standard tick marks.		
32	The solution must have the capability to write supervisory review notes with links to targeted working papers.		
33	The solution supports file attachment and review notes		
34	The solution has a robust process for approval of the work papers and audits. The system allows for auditors to transfer their work papers to the manager's review at any time and allows for the manager to be automatically notified that a working paper is waiting for a review.		
35	The solution must have the capability to print completed working papers including audit programs and review notes.		
T	Reporting:		
36	The solution must support the generation of audit reports in multiple formats, including interactive dashboards and real-time collaboration features.		

37	The solution must have the capability to customize audit report formats at any time for future requirement changes		
38	The solution must have the capability to maintain tracking of changes of supervisory review of reports		
39	The solution supports sending the draft report to Auditees for their comment		
40	The solution must have the capability to issue final reports to the authorized person for approval		
41	The solution must have the capability to receive more than one management response for each Issue		
U	Follow-Up:		
42	The solution must have the capability to automatically capture the audit recommendations from the audit report.		
43	The solution must have the capability to enable auditees to access (web-based mode) and capture the actions taken by themselves for Issues addressed to them.		
44	Does the solution have the capability to enable auditees to access (web based mode) and capture the actions taken by themselves for Issues addressed to them. The system allows for action plans to be reviewed and approved by a specified reviewer or issue coordinator, and the status of action plans to be tracked.		
45	The solution must have the capability to track and automatically follow up all pending Issues, on a web-based mode and through sending out e-mails		
46	The solution must have the capability to search open Issues per Audit Assignment based on user defined parameters.		
47	The solution must have the ability to offer the ability to track and follow up multiple management responses and by addressees.		
V	Administration:		
48	The solution must have the capability to capture Internal audit staff profile like education, work experience, skills, Certifications, etc.		
49	The solution must have the capability to enable supervisors to complete auditor performance evaluation for specific audit assignment/project		
50	The solution must have the ability to offer the ability to determine automatically when a specific auditable area was last audited and the auditor performing the audit.		
W	Survey and Assessment:		
51	The solution must have the ability to possess technology to send surveys to auditees, obtain comments, summarize results.		

52	The solution must have the capability to conduct customer satisfaction surveys and other critical surveys with various stakeholders.		
53	The solution must have the capability to create dashboards to provide summarized audit data for management and the Audit Committee of the Commission.		
54	The solution must have the ability to publish surveys/questionnaires online via a web application to auditees.		
Third party risk management			
55	Vendor Onboarding: Implement a structured onboarding process for new vendors with workflow enabled.		
56	Due Diligence - Financial Stability: Assess the financial stability of vendors to ensure they can meet their obligations.		
57	Due Diligence - Legal Compliance: Verify that vendors comply with all relevant legal and regulatory requirements.		
58	Due Diligence - Reputation: Evaluate the reputation and past performance of vendors through references and industry feedback.		
59	Due Diligence - Operational Capability: Assess the operational capabilities of vendors to ensure they can deliver the required services or products.		
60	Due Diligence - Security Posture: Evaluate the security measures vendors have in place to protect data and systems.		
61	Contractual Agreements: Allow the capability to attach contracts and evaluate them using workflow		
62	Vendor Catalog - Maintaing a list of all vendor, their services & details of internal function, stakeholder ownership.		
63	Vendor Risk Register: Maintain a detailed risk register for all vendors, documenting identified risks and mitigation plans.		
64	Third-Party Tools Integration: Integrate with third-party tools for real-time vendor monitoring and risk assessment.		
65	Risk Mitigation Plans: Develop and implement risk mitigation plans for identified vendor risks.		
66	Incident Management: Establish clear procedures for vendors to report and manage incidents, including data breaches.		
67	Access Control: Ensure vendors implement strict access control measures to limit access to sensitive information.		
68	Termination Procedures: Define procedures for the orderly termination of vendor relationships, including data return or destruction.		
69	Vendor Risk Scoring: Implement a risk scoring system to categorize and prioritize vendors based on their risk levels.		
70	Survey Capability for Vendor with a Tool that can be deployed and Managed On-Prem.		
71	Survey tool must not need Vendor to create login/access in system - to avoid exposing the bank to risk or vulnerabilities.		
General Requirements			

72	Must be able to support multiple database such as MS SQL, Oracle, MySQL.		
73	Must have ability to be deployed in cloud or on premise.		
74	In view if the regulatory expectations, as a mandatory requirement for bank, the system must have advanced reporting capabilities and functionality to produce reports in the following formats: MS Power Point, MS Word, MS Excel, and PDF.		
75	Must have flexible dashboarding capabilities. The system should also allow users to create custom dashboards with drag-and-drop functionality and real-time data integration from various sources.		
76	The platform must be a no-code/low code configuration tool. The platform should include a built-in library of pre-configured templates and workflows that can be customized with minimal technical expertise.		
77	The platform must allow configuration of unlimited number of pages or screens to meet the functional requirements, without the bank having to procure additional licenses for modules or applications on-demand		
78	Flexibility: The system shall be configurable and provide technical flexibility that allows to update configuration or add additional fields without customization through programming and customized code or requiring professional services for customization.		
79	The system should incorporate an ETL feature to extract, transform, and load information asset data from other systems.		
80	The system should also include granular access controls with the ability to define permissions at the data field level, along with audit logging of all access changes.		
81	The system must allow configuration of dynamic business workflows.		
82	In view of Regulatory guidance, the system must allow for multi factor authentication.		
83	In view of the expanding scope of information security operations and the department as a whole, the GRC tool may need to have extensive integrations and data management capabilities. As such it is mandatory for the platform to have in build ETL capabilities.		
84	The system should have notification capabilities based on pre-defined business criteria.		
85	Audit trail history logs.		
86	Multitude of layout options and templates without the need the need for custom coding.		
87	Meticulous support of user access rights and the ability to modify user access rights based on employee roles and at stages during the life cycle.		

RFP for Supply, Installation and Maintenance of
Cybersecurity Solutions and Associated
Hardware at the Bank

88	Configurable search functionality.		
89	Ability to provide comprehensive dashboards and reports which provide snapshots and meticulous details		
90	Support both upload and download of data in various formats.		
91	All system tables should have advanced filtering capabilities.		

Technical Specifications for Decoy (Honeypot)			
S No	Minimum Technical Specifications	Vendor's Compliance	Vendor's Remark
A	General Requirements		
1	The proposed solution must be cloud-native with optional hybrid deployment, supporting both cloud and on-prem components for flexibility in deployment scenarios.		
2	The solution must support encryption in transit and at rest, with compliance to industry standards such as FIPS 140-2, ISO 19790 or any other equivalent standard, ensuring secure integration with the bank's infrastructure.		
3	The system must allow for the estimation of Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objectives (RTO), and Recovery Point Objectives (RPO) for each business process.		
4	The solution should include automated response capabilities, such as sandboxing, isolating, or diverting attackers, with customizable containment policies and integration with SIEM and SOAR tools.		
5	To ensure the maturity and stability of the platform, all the features and functionalities of the proposed solutions must be present from day one.		
6	Decoy solution should be able to replicate Bank's existing infra components or similar components.		
7	Solution should comprise of low interaction honeypot, medium interaction honeypot as well as high interaction honeypot. The solution should be capable of providing both virtual and physical honeypots. The solution should provide firewalls decoy, IDS/IPS decoy, WAF decoy & MZ decoy for LB, web server and a separate DMZ to deploy decoy Application and DB servers.		
8	VMs with Windows, Linux, Unix (different flavors) server can be used as part of solution to simulate such trap environment.		
9	Solution deployment must ensure that, it should be near impossible for the attacker to differentiate amongst real and trap systems (decoys).		
10	It should be able to capture network scanning attempts, application vulnerability exploitation, OS scan, Malwares, malicious file hashes, system hijack etc.		
11	The decoys should be scientifically placed in multiple subnets, so the hackers will encounter them in the process of trying to find valuable information. When the hackers try to access the decoys, a silent alert should be raised, and full forensics related to the attack should be collected. Decoy should be able to capture details such as attack vector used, attack methodology, tools used for attack, source of the attack etc		
12	The solution based on the learnings should suggest solution to mitigate the risk.		

13	The decoy should act as real servers, desktops, files, users accounts, applications like SWIFT/NEFT/RTGS/Core banking, Internet Banking, Mobile Banking, Loan Systems, ATM Switch and any other system available in the Banks overall IT ecosystem by using them as traps.		
14	The solution should identify signature, behavior patterns and should also provide effective approach in detecting advanced attacks including malware-less attacks, bot attacks etc. that can circumvent existing preventive controls.		
15	The proposed Deception solution should be seamlessly integrate with the Bank's Active Directory and with SIEM solutions and should provide monitoring and network visibility as well as early detection of attacks while keeping false positives to almost nil as well as any other security solutions so as to take intended action to block or take action against the affected assets and any other existing or future solution, as required by the Bank.		
16	Solution should be able to generate actionable intelligence and should be able to integrate with existing threat intel platform		
17	Solution should have Centralized Management Console with customizable dashboard and role-based admin.		
18	In case of complete compromise of decoy solution, it should still not be able to launch attack on to the other system within the environment.		
19	Ability to detect all types of attack vectors including but not limited to: pre-attack reconnaissance, zero-day attacks, privilege escalation, lateral movement and data-theft		
20	The solution must have the ability to visually replay past events on an interactive fluid dashboard that show all decoy elements and attacker details.		
21	Solution must allow visual dissection of the PCAP traffic and preserve all network traffic to and from the decoys while having the ability to export PCAPs based on a time filter.		
22	Solution must use a numeric risk score for an attacker based on dynamic analysis of attacker behavior.		
23	The system must have the ability to save and share custom views filtered based on time and any event metadata for analyzing specific events. Results of saved queries must be exportable.		
24	The solution must have the ability to reconstruct raw attack data into plain English attack analysis. It must also provide attacker / APT group attribution, mitigation recommendations, MITRE mapping within the user interface for the analyst.		
25	Measures to enhance deception strength of decoys should be in place like- Decoys should be integrated with the real Active Directory domain and should not use a domain trust relationship between a dummy Active Directory and the real Active Directory domain that hackers can easily discover.		
26	Ability to embed lures on real endpoints, without using an agent, in the form of unique dummy credentials that lead attackers on to decoy systems. They must be able to trigger action on Bank defined and configurable activities.		

27	The solution must support geo location of external threats.		
28	Deception platform should automatically fill network decoys with realistic auto-generated enticing content containing folders and files pertaining to all business verticals. The number of folders and files to generate and the file creation dates (oldest to newest) should be configurable. The files generated should be a combination of terms relating to specific verticals as well as predefined keyboards defined by organization.		
29	Real times alerts to be generated via email and user console, based on preset or custom notification rules.		
30	For security, the base operating platform (host operating platform on which the decoys run) of the deception appliance should not be on Linux or Windows which are prone to regular remotely exploitable vulnerabilities.		
31	When an event occurs, the solution should have built in orchestration to take specific actions based on preset or user specified rules that can be specified on any event meta-data. The rule engine should support multiple Boolean and logical conditions to appropriately orchestrate the response. (Ability to integrate with GRC tool and SOAR platform may be also made a part of the same, to void duplicity and effectiveness of counter response)		
32	Decoys must be very robust and shall never interfere with business functions/ objectives of the setup where they are placed.		
33	Honeypot should be able to store attack data, visualize attack data. It should have capability of threat hunting and search (CVE-Search, IP based search, Port based search, Hash value based search etc.)		
34	Solution should be able to generate customized reports (monthly, weekly, daily etc.), dashboards etc.		
35	Placement within DC & DR		
36	Solution must provide built in signature detection for 'known bad' events and must be updated with the latest emerging threat signatures.		
37	Decoys created should be added as computer objects to the real Active Directory domain and should not use a domain trust relationship between a dummy Active Directory and the real Active Directory domain that hackers can easily discover.		
38	Deception platform must be capable of creating file decoys that are deployed on real systems and agentlessly trigger alerts not only when opened but also when copied, modified and deleted		
39	The solution should have the ability to capture commands executed for hi-interaction SSH connections on Linux decoys without any instrumentation processes or agents running within the decoys.		
40	Deception platform should automatically fill network decoys with realistic auto-generated enticing content containing folders and files pertaining to specific business verticals like Finance, Legal, HR, IT etc. The number of folders and files to generate and the file creation dates (oldest to newest) should be configurable. The files generated should be a combination of terms relating to specific verticals as well as pre-configured keywords related to the organisation.		

41	The solution must include integrated sandboxing capabilities for detonating malwares and files that are being used as part of the attack		
42	Solution should support ability to deploy a Windows Active Directory server as a target instance or integrate the decoys and deceptive Page 55 of 67 users with the production AD. Should have the ability to create deception in the Active Directory (AD), without using the real AD instead of a dummy AD / trust relationship.		
43	The solution should be capable of mimicking other devices like printers, switches, routers, Voice over IP phones and Video Cameras		
44	Solution should support download of all endpoint deceptive object information in CSV file		
45	Solution should be capable to integrate with firewall on API and isolate the endpoints that are being used for attack or botnet using automated rules.		
46	The solution should have the capability to deploy clients for endpoints spread across branches all over India, through a central tool.		
B	Solution Capabilities		
47	The decoys created should be added as computer objects to the real Active Directory domain and should not use a domain trust relationship between a dummy Active Directory and the real Active Directory domain that hackers can easily discover.		
48	The deception platform must be capable of creating file decoys that are deployed on real systems and trigger alerts not only when opened but also when copied, modified and deleted		
49	The solution should capture commands and keystrokes with minimal performance impact, using lightweight, agent / agentless techniques that do not alter the decoy's behavior.		
50	The solution must support the creation of custom decoy templates via an intuitive interface, with options for A/B testing to optimize decoy effectiveness against different attacker profiles.		
51	The proposed solution should have the ability to create specialised internet facing decoys to detect external reconnaissance of internet facing websites. These decoys should only respond to requests on HTTP/HTTPS and only for their requests to the configured domain names. Also, the solution must include advanced analytics for external decoys, capable of identifying and categorizing reconnaissance techniques, and integrating with external threat intelligence feeds.		
52	For authenticity, Linux high-interaction decoys should be one-to-one (the solution should not re-use of a few internal VMs configured with multiple IPs to show multiple decoys).		
53	The solution must have the ability to embed lures on real endpoints in the form of unique dummy credentials that lead attackers on to decoy systems		

54	The endpoint deception agent should be able to deploy custom endpoint decoys on different types of end-users. For this, the solution should be able to identify different types of users (finance/IT/legal/HR/marketing etc.) based on the combination of following selection criteria:		
55	- Process list on the user's machine		
56	- Browser history		
57	- Installed programs		
58	- Interesting files		
59	- Recent commands		
60	- Hostname (Specific/RegEx)		
61	- OU that the user belongs to		
62	All Windows high interaction activity should be logged, not just code execution attempts. High-interaction should not involve transfer of malicious code to a separate analysis VM, but should provide full interactive access to the attacker.		
63	The deception platform should automatically fill network decoys with realistic auto-generated enticing content containing folders and files pertaining to specific business verticals like Finance, Legal, HR, IT etc. The number of folders and files to generate and the file creation dates (oldest to newest) should be configurable. The files generated should be a combination of terms relating to specific verticals as well as pre-configured keywords related to the organisation.		
64	The solution should be able to create multiple decoys with RDP access and show only one network Interface in system settings under Windows when connected over RDP.		
65	The SSH decoys should show the same IP under ifconfig as the one used to connect via the SSH client.		
66	The system should offer customizable templates for various types of exercises, including integration with external simulation tools, for tabletop exercises, walkthroughs, simulations, and full-scale drills.		
67	The solution should have the ability to create decoy application in the standard cloud environments such as decoy User, Service Principal, Managed Identity, App Service, Storage Account Container, Storage Account File Share, Key Vault, ARM Template, Container Registry and VM Image		
68	The proposed solutions should have the ability to detect and defend against identity-based attacks such as credential theft and privilege abuse, Active Directory assaults, and risky entitlements in real-time.		
69	In order to eliminate the attack surfaces, the proposed solution must support application access through outbound service initiated connections (unidirectional inside-out connections) i.e., it should not require any inbound firewall rule from OEM's cloud platform and only outbound traffic should be allowed.		
70	The connectivity between users' devices and private applications must be through encrypted tunnel and optimally routed through the nearest data centres with lowest possible latency		

71	The decoy connectors must operate in high availability (HA) and support built-in load balancing		
72	The solution must have AI-powered engines for automatic discovery of internal applications/servers to easy policy creation		
73	The system should generate BCM reporting in various formats including MS Word, PowerPoint, Excel, PDF, and HTML with necessary branding as per Bank's expectation.		
74	For additional security, the endpoint agent must not use global password for logout, disable individual services, exit, and uninstall.		
75	The endpoint agent must support all the leading OS like Windows, macOS, Linux, Android, iOS etc		
76	As a mandatory security requirement, the endpoint agent must be turned on as soon as the device boots up		
77	The solution must support at least 5 devices (Desktop/Laptop/Mobile/Tablet etc.) for a single authenticated user		
78	The solution must have the ability to universally define, deploy, and immediately enforce policies for all users, across all locations from a single console. The policy updation must be in real-time		
79	The solution should protect internal applications from external attacks. Even if there are some vulnerabilities on the application, it should not be exposed		
80	The solution should have the ability to stream the access logs to multiple on-premise SIEM solutions		
81	Whenever issues get reported by end-users, packet capture is required for diagnosis, hence the endpoint agent must have built-in packet capture feature from the day one for troubleshooting		
82	The endpoint agent must have inbuilt debugging capabilities and should have an option to report an issue to technical assistance centre (TAC) directly from the endpoint agent console		
83	The proposed solution must do the endpoint policy checks at regular intervals and not just at the time of initial user authentication/authorization		
C	Administration, Manageability and Reporting		
84	The solution should utilize AI/ML-based behavioural analytics to dynamically adjust risk scores, incorporating historical data and real-time threat intelligence.		
85	The solution must have the ability to reconstruct raw attack data into plain English attack analysis. It must also provide attacker/APT group attribution, mitigation recommendations, MITRE mapping within the user interface for the analyst.		
86	When an event occurs, the solution should have built in orchestration to take specific actions based on preset or user specified rules that can be specified on any event meta-data. The rule engine should support multiple boolean and logical conditions to appropriately orchestrate the response.		
87	The solution must have the ability to visually replay past events on an interactive fluid dashboard that show all decoy elements and attacker details.		

RFP for Supply, Installation and Maintenance of
Cybersecurity Solutions and Associated
Hardware at the Bank

88	The solution must allow visual dissection of the PCAP traffic and preserve all network traffic to and from the decoys while having the ability to export PCAPs based on a time filter.		
89	The solution supports native integrations with global TI feeds like AbuseIP, Ipinfo, Virustotal, Cisco tallos etc.		
90	The solution should have a central management console to manage the deployment and event notifications. All other components should be controlled and configured through the central management console only.		
91	The solution must have the built in ability for real-time email alerts based on preset or custom notification rules		
92	The solution should have automatic backup/restore of events and configuration data, with no manual intervention required from the customer.		

Technical Specifications for Mobile Device Management			
S No	Minimum Technical Specifications	Vendor's Compliance	Vendor's Remark
A	Support		
1	MDM solution must Support Android OS 6 and above		
2	MDM solution must Support iOS 12 and above		
3	MDM solution must Support SAFE/KNOX, ADO, Supervised(iOS) APIs		
4	MDM solution should support Zero Touch Enrollment.		
5	MDM solution should support integration with Google's Android Enterprise		
6	MDM solution should be Google Compliant and available on Google Play Store.		
7	MDM Solution should be Android Enterprise Certified.		
B	Mobile Device Management		
8	The MDM solutions should have a product tour for the Admin Console when admin logs in for the first time		
9	The MDM solutions must be able to see statistics of OS(Android and iOS) version on devices in realtime on dashboad		
10	The MDM solution must be able to see statistics of device MDM agent version in realtime on dashboad		
11	The MDM solution must have Over the Air Device Enrollment (via email, SMS, QR code, bulk enrollment)		
12	The MDM solutions must have Device naming convention for Bulk Enrollment		
13	The MDM solutions must have Push Wi-Fi setting		
14	The MDM solutions must have Configuration monitoring/auditing and ensure audit logs are immutable and tamper-proof		
15	The MDM solutions must have Automated provisioning/enrollment and de-provisioning based on criteria		
16	The MDM solutions must be able to disable camera -Bluetooth -NFC - Screen Capture - Airplane Mode - Cellular data - Hotspot - Wi-Fi		
17	The MDM solutions must be able to block USB - Factory Reset from Device Setting and block USB for data transfer while allowing charging.		
18	The MDM solutions must have admin role based privileges and also have support for custom roles and Permissions		
19	The MDM solutions must be able to generate report of Location Tracking (Historical)		

20	The MDM solutions must be able to locate devices on a single map: 1. Showing all devices location on single map 2. Selecting devices and showing their location on single map 3. Selecting groups and showing the location of all devices in that group on single map		
21	The MDM solutions must have Block mounting physical media		
22	The MDM solutions must have Block Primary Microphone		
23	The MDM solutions must be able to Block SMS/ MMS/ Outgoing calls		
24	The MDM solutions must have the option for the admin to change the Company Name and logo on the Web Console portal.		
25	The MDM solutions must have Policy for USB Debugging, location, device accessibility,etc.		
26	The MDM solution should provide option to configure policy for Android Device OS update management		
27	The MDM solution should support Android Management API (AMA)		
28	If a device is not compliant with the security policies and compliance rules put in place by the Android Management API, the use of business data should be automatically restricted.		
29	The MDM solutions must have the option to enter IMEI on Device overview page for the devices having Android 10 and later versions.		
C	Device Health Monitoring		
30	The MDM solutions must be able to see non-complaint devices alert on dashboard		
31	The MDM solutions must be able to see blocked devices statistics on dashboard		
32	The MDM solutions must be able to see last synced data of devices to server/console on dashboard		
33	The MDM solutions must be able to view Device battery percentage on dashboard		
34	The MDM solutions must be able to view Device storage capacity on dashboard		
35	The MDM solutions must be able to view Device manufacturer details on dashboard		
36	The MDM solutions must be able to view threat statistics (malwares, viruses, etc.) on dashboard		
D	Mobile Application Management		
37	The MDM solutions must be able to track app inventory		
38	The MDM solutions must Be Able to do Custom App Distribution		
39	The MDM solutions must be able to distribute Playstore/App Store apps		
40	The MDM solutions must be able to track App Usage		
41	The MDM solutions must be able to see most installed apps on dashboard		

42	The MDM solutions must be able to do Application blacklisting/whitelisting		
43	The MDM solutions must be able to do Application category blacklisting (eg. Social Networking, Media etc.)		
44	The MDM solutions must be able to manage app versions		
45	The MDM solutions must be able to Install, update and remove managed apps from a device remotely		
E	Manage "Enterprise Apps Store"		
46	The MDM solutions must be able to Restrict new App installation		
47	The MDM solutions must be able to Restrict apps		
48	The MDM solutions must be able to Block App Installation from Unknown Sources		
F	Mobile Security Management (MSM) and Mobile Threat Management (MTM)		
49	The MDM solutions must have Anti Virus with Malware Detection with indigenously built AV engine		
50	Must be able to do Scheduled Scan / Real Time Scan		
51	The MDM solutions must have Password protection for devices as policy		
52	The MDM solutions must be able to selectively wipe device remotely (factory reset, complete wipe, wipe particular path, file extension-based wiping)		
53	The MDM solutions must be able to selectively wipe device remotely (factory reset, complete wipe, wipe particular path, file extension based wiping)		
54	The MDM solutions must be able to do Device compromise detection (jailbreak/rooting)		
G	Virtual Fencing		
55	The MDM solutions must be able to do Geo Fencing, Wi fi Fencing & Time Fencing		
56	The MDM solutions must be able to apply multiple fences in one policy		
57	The MDM solutions must be able to allocate relation (AND/OR) between multiple fences applied in a policy		
58	The MDM solutions must be able to log event on fence/s trigger		
59	The MDM solutions must be able to update Policy/Profile on device based on Fence/s trigger event		
H	Network management		
60	The MDM solutions must able to do Data usage Monitoring of device (segregated by Mobile data, wifi data, roaming data) logged for each day		
61	The MDM solutions must able to do Data usage Monitoring by application (segregated by Mobile data, wifi data, roaming data) logged for each day		
62	The MDM solutions must able to show top Apps using most data on dashboard		

63	The MDM solutions must be able to show top Devices using most data on dashboard		
I	Analytics		
64	The MDM solutions must be able to perform global search anywhere within the Admin Console		
65	The MDM solutions must have provision for Alerts and notifications		
66	The MDM solutions must have facility to enable notification via email and/or in-console		
67	The MDM solutions must have real time dashboard		
68	The MDM solutions must have dashboard widget for Agent unauthorized removal		
J	Reporting Module		
69	The MDM solutions must have on-demand reports for the following:		
	1. Device Compliance Report		
	2. Device Health Report		
	3. Device Asset tracking report		
	4. Device Connected Report		
	5. Malware Detection Report		
	6. Internet Data Usage Report		
	7. Call/SMS logs Tracking Report		
	8. App Non-compliance Report		
70	The MDM solutions must be able to do Customized Reporting		
71	The MDM solutions must be able to add filtering criteria to custom reports (eg, equals, not equal to, contains, does not contain, start with, end with, less than, greater than, in, not in, between)		
72	The MDM solutions must be able to apply aggregating functions (count, average, sum, maximum, minimum) in reports		
73	The MDM solutions must be able to apply custom column names within reports		
74	The MDM solutions must be able to schedule the Reports (monthly, weekly, daily, etc)		
75	The MDM solutions must be able to do Device and Application Level Analytics		
76	The MDM solutions must have Export reports/ device data in CSV format to be consumed by other enterprise tools		
77	The MDM solutions must have proactive notification on Web-console and/or via Emails in case of any non-compliance		
K	Advanced Features		

78	The MDM solutions must have facility to lockdown device to a few selected/permitted apps (all other apps on device are inaccessible)		
79	The MDM solutions must have facility to lockdown device to few selected/permitted apps (all other apps on device are inaccessible)		
80	The MDM solutions must have facility to upload branding wallpaper and company logo		
81	The MDM solutions must be able to do files broadcast		
82	The MDM solutions must be able to do Message Broadcast to all users		
83	The MDM solutions must be able to monitor Call And SMS Log		
84	The MDM solutions must be able to monitor Admin Action log for audit purpose		
85	The MDM solutions must be able to monitor Activity log for audit purpose		
86	The MDM solutions must be able to have Group Level Administration facility		
L	Service Management		
87	Solution should have the option of Remote control to manage Android Devices & Screen Mirroring for iOS devices.		
88	The MDM solutions must be able to do Remote transfer of File during remote control of device		
M	Web Security		
89	The MDM solutions must have the capability to do URL Blacklisting/Whitelisting on browser		
90	The MDM solutions must have the capability to category Wise URL blacklisting/whitelisting on browser		
91	The MDM solutions must have the capability to do URL Blacklisting/Whitelisting by category and based on keywords		
92	The MDM solutions must have the capability of Browsing and Phishing protection		
93	The proposed solution should provide tight integration with Bank's Email Solution.		
94	C-SOC (Cyber Security Operations Centre) Solutions and other existing solutions / related infrastructure in Bank with capability of Conditional access.		
95	The proposed solution should be configured and scalable to cater the requirement of implementation of the solution. The solution deployment should be compliant with Bank's IS, IT and Cyber policies, internal guidelines, regulatory requirements and country wide regulations and laws from time to time.		
96	The proposed solution should be able to support 1 device per license, which can be customised based on the different groups created for various users to assign different policies to them.		
97	The proposed solution should have tight integration with existing content systems and with group-based security and remediation policies.		

98	The solution should have the capability to integrate with the following:		
99	a)Native Applications		
100	b)Active Directory		
101	c) Bank's Email Solution		
102	The MDM solution should have an option to display Bank's logo/name/icon in back ground.		
103	The proposed solution should support version upgrades/patches to applications on demand by user.		
104	The proposed solution should allow whitelisting/blacklisting of applications so that only whitelisted applications are allowed to run and blacklisted applications will never be installed.		
105	The proposed solution should provide built in multi factor authentication.		
106	The solution proposed should ensure device-binding feature for mail i.e the user can access mail from authorised/MDM enrolled device only.		
107	The proposed solution should have capability to limit the device registration & Admin can uninstall unapproved devices.		
108	The proposed solution should have capability to authenticate users against passcodes, 2FA, etc.		
109	The proposed Solution should Create and distribute customized policies and license agreements.		
110	The proposed solution should apply and update default device policy settings.		
111	The proposed solution should have capability to Approve or uninstall new mobile devices on the network based.		
112	The proposed Solution should have ability to restrict device features such as camera, screen capture, cloud backup etc while maintaining user's privacy intact.		
113	The proposed solution should have ability to enforce kiosk mode features. Kiosk mode means to restrict device to run approved applications only.		
114	The proposed solution should have Privacy features to block sharing of information from containerized areas.		
115	The proposed Solution should have capability to send commands (such as device query, clear passcode, send message, lock device, set roaming, remote view, sync device) on demand to devices to request information and perform actions / commands.		
116	The proposed solution should have capability to Remotely locate, lock and wipe lost or stolen devices; selectively wipe corporate data while leaving personal data intact.		
117	The proposed solution should support creation of policies & accordingly display the compliance.		
118	The proposed solution should support automatic policy control that deletes all enterprise policy, apps, and data if MDM agent is uninstalled/removed.		

119	The proposed solution should have the capability to push policies using web interface and should not rely on use of scripting.		
120	The proposed solution should provide a centralized event log tool that captures logs from all devices and administrative events (logging, policy changes, application updates, configuration updates etc.)		
121	The proposed solution should manage Wi-Fi supporting and non-cellular devices as well with equal policy compliance.		
122	The proposed solution should be able to define policies by device or Group.		
123	The proposed solution should support checking of device policy compliance before allowing enterprise resource accesses and should support and enforce user authentication before device use.		
124	The proposed solution should record both device and console events for integrated devices to capture detailed information for system monitoring, and provide logs view in the console and export the reports.		
125	The proposed solution should have the ability to customize MDM policy to be in line with the Bank's policies such as password policy, manage groups of devices.		
126	The proposed solution should have capability to grant or restrict document access from outside the container.		
127	The proposed solution should have capability to prohibit applications installed on the device.		
128	The proposed solution should provide alerts via email/reports on encountering below scenarios (but not limited to):		
129	i. Device has not connected in a period of time		
130	ii. Device has outdated policies		
131	iii. Device has an installed application that is on the disallowed applications list		
132	iv. Device has an installed application that is not on the allowed applications list		
133	v. Device does not have an application that is on the required applications list		
134	vi. Device has uninstalled a previously installed required application		
135	The list of apps will be as per the business requirement of the Bank.		
136	The proposed solution should have feature of User(s) and Group Management.		
137	The proposed solution should have capabilities of:		
138	a) Corporate Application Management.		
139	b) corporate content / Data management.		
140	c) Device Management.		
141	d) Data Centric Security ensuring containerization of Corporate Content / Data.		

142	e)	Encryption of Container for Security and password protection.		
143	f)	Viewing location information on lost / stolen Mobile devices.		
144	g)	Remote locking of Mobile device(s).		
145	h)	Detecting Jailbreak / Root mechanism.		
146	i)	Custom Reports and Analysis.		
147		The proposed solution should ensure that Business data doesn't get copied to personal data or any 3 rd Party email system. The solution should provide segregation of private and corporate data such that corporate data cannot be copied from the device via mass media storage.		
148		The proposed solution should support selective wiping of only Business data from a lost / stolen device.		
149		The proposed solution should push user-specific device configuration / Organization's Policy Deployment.		
150		The proposed solution should obtain supported device(s) information by hardware model, serial number, UDID etc.		
151		The proposed solution should support all Operating Systems (Android, iOS) over wide category of Mobile Devices such as iPhone, iPad, Tablets, Android based Mobiles etc.		
152		The proposed solution should provide Malware and Virus protection.		
153		The proposed solution should provide an option for performing tasks related to Pin, Password, or biometric Access reset remotely for Mobile Devices. The Dashboard should provide status of Devices enrolled, along with the inventory.		
154		Solution should be able to Secure BYOD and Corporate provided mobile devices.		
155		Solution should be able to perform Mobile Application Management to restrict data leakage from authorized and protected apps to unmanaged apps.		
156		Enforce device enrolment to Mobile Device Management and Mobile Threat Defense Solution before allowing access to corporate resources.		
157		The proposed solution should prevent manual override of MDM policies by mobile device user.		
158		Solution should be able to publish internal web apps securely and allow access to only domain joined or registered mobile devices.		
159		Solution should be capable of advanced security solution for various flavours of OS that helps protect against threats, vulnerabilities, behaviors, and configurations originating on mobile devices.		
160		The proposed solution may have capability of remote control devices when providing end user support.		
161		The proposed solution should manage and deploy apps based on pre-defined groups and/or as per Policy of Bank.		

162	The proposed solution should be capable of remote up gradation of OS / Applications and deployment of patches to them.		
163	The proposed solution should be capable to activate and update agents by manual or over-the-air (OTA) installation.		
164	The proposed solution should be able to block connections to untrusted networks.		
165	The proposed solution should be capable of applying granular level restrictions on data.		
166	The proposed solution should support Enterprise app store to upgrade existing application as well as download new apps.		
167	All the Hardware & Software supplied under this contract should be TLS 1.3 or higher Ready.		
168	The Mobile Threat Defense solution should protect devices from phishing and the wide range of application, device, and rogue network originated threats.		
169	The Mobile ThreatDefense Solution should prevent malicious cyber attacks such as :		
170	A) Man in middle attacks		
171	B) Reconnaissance scans		
172	C) OS/Kernel Exploitation		
173	D) Profile/Configuration Changes		
174	E) System tempering		
175	F) Known/unknown malware		
176	G) Malicious apps		
177	Data at rest and data should be in encrypted container and secured and should not allow copying data outside container.		

Technical Specifications for Secure Backup and Ransomware Protection

S No	Minimum Technical Specifications	Vendor's Compliance	Vendor's Remark
1	Bidders must provide advanced ransomware protection, including Cyber Attack or data corruption for Bank's Oracle Databases		
2	Must have real-time data protection ensuring near-zero (until the last sub-second) data loss, with granularity down to the last transaction		
3	Must offer end-to-end immutable solution, from backup creation on local appliance, to replica in DR site, and to storage – all centrally managed and tracked by Enterprise Manager across the entire database environment		
4	Recovery Assurance through continuous validation, with automated alerts for anomalies during data ingest and at rest		
5	Must ensure that all data validation, backup integrity checks are performed at proposed appliance level, no Production Server resources are used		
6	Solution must be able to send only incremental data to the proposed Appliance thereby avoiding recurring full backups.		
7	Solution must validate the incoming changed data blocks, and must compress, index and stores them in Appliance.		
8	Solution must have ability to provide Virtual Full Database Backups, which are space-efficient pointer-based representations of physical full backups.		
9	Dashboard view of Recovery Window and RPO of all configured Database		
10	Fast and granular data recovery at any given point in time, with options for data files, or tablespaces or Database block as per defined policy		
11	Must be sized to handle Oracle Database workloads with minimum of 500 TB usable capacity and scaleable up to 1PB within same rack, with capability for future expansion		
12	Must be able to compress and encrypt TDE (Transparent Data Encryption) encrypted Oracle DB backups, ensuring security and space optimization		
13	Data in transition must be encrypted using SQL*Net & TLS encryption, Solution must follow all of NIST's (National Institute of Standards and Technology) best practices for a Zero Trust Architecture		
14	Appliance must provide multi-factor authentication (MFA) and quorum-based authorization for admin access		
15	Separation of duties architected into the security framework with role-based access controls (RBAC) for database, backup, and storage administrators		

RFP for Supply, Installation and Maintenance of
Cybersecurity Solutions and Associated
Hardware at the Bank

16	Should include automatic corruption detection during the first full backup and subsequent incremental backups, with automated repair and notification features		
17	Must offer periodic comprehensive single bundled patch updates for proposed backup solution (including hardware and software components), with a clear schedule and rollback options		

Technical Specifications for **Network Access Control**

S No	Minimum Technical Specifications	Vendor's Compliance	Vendor's Remark
1	The solution must provide Authentication, Authorization and Accounting (AAA) services, Profiling, Posturing, Guest Management from a single platform.		
2	The solution should be software based (VM) / Appliance Based		
3	The solution should authenticate and authorize users from wired, wireless & VPN network		
4	The Solution shall use Agent based approach for Desktops, Laptops, etc. and Agentless for other devices including Network Devices, Printers/Scanners, Wireless access points, etc., for detection of unauthorized access via network activities analysis from the endpoints		
5	The solution should support 802.1x authentication for domain joined devices for wired & wireless network		
6	The solution should support MAB authentication for headless devices like Printers,scanners,IP phones etc. Solution should support google auth, AD and SAML2 authentication.		
7	The solution should be able to block unauthenticated/ rogue machine without giving any access to the network. The solution should be able to control the user even before IP address is assigned. It should act as a pre-admission solution(802.1x)		
8	The solution must support agent-based / agentless deployment and provide deep compliance check for Meeting regulatory compliance requirements of RBI, ISO 27001, other Government bodies etc. revolve around knowing "who, what, when and where" for devices and users on your network and controlling access to the data your company needs to keep secure.		
9	The solution should dynamically profile endpoints discovered on the network, based on the configured endpoint profiling policies, and automatically assign respective endpoint attributes		
10	The solution should use a combination of techniques like DHCP, browser data, MAC addresses, network devices, external databases etc to track and identify devices on a network or web environment		
11	The solution should dynamically authorize endpoints based on user group, profile & posture properties to respective vlan or network		
12	The solution shall be a vendor-agnostic solution suited for heterogeneous networks.		
13	The solution should support authentication protocols including PAP,MS-CHAP,PEAP and EAP-TLS and 802.1X Single Sign-On (SSO)		
14	The solution should be able to profile IoT /IIoT devices and assign relevant network		
15	The solution should integrate with AD/LDAP server for authentication		

16	The solution should provide wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect or equivalent.		
17	The Solution should support the following endpoint checks for compliance for windows endpoints		
a	Check operating system/service packs/hotfixes .		
b	Check process, registry, file & application .		
c	Check for Anti-malware installation/Version/ Anti-malware signature Definition Date		
d	Check for windows update running & configuration		
e	Check domain joined or not		
f	Execute custom scripts		
g	Check Vulnerable applications installed		
18	The solution should provide Deep Compliance checks on from Day one.		
a	Check Specific Anti-malware product version and last signature update date		
b	Threats detected by the installed Anti-malware product with option to configure threat exclusion.		
c	Disk Encryption status of System & Local volume Encryption tool & its version.		
d	DLP application status		
e	Local firewall status		
f	EOL status of device operating system and last operating system update. Enforce policies based on the update availability		
g	Detect Browser extensions		
h	Maintain a inbuilt database of list of Potentially unwanted Application(PUA) and detect them		
i	Ability to create playbooks to run specific tasks on endpoint and assign compliance status		
j	Anti-phishing protection setting on default or all web browser installed		
19	The solution should provide the enduser to request for temporary access incase of authentication/authorization failure that can be approved by a admin		
20	The solution shall provide self-enrollment of devices		
21	The solution should allow endpoint details to be added to a group manually or by bulk upload using csv file type		
22	The solution should provide Guest onboarding both self and sponsored		
24	The solution should be able to publish contextual intelligence to 3rd party devices		
25	The solution should provide threat enforcement based on the threats detected by external systems without any additional agents & quarantine the endpoints		
26	The solution should support distributed deployment options with clustering of nodes with a central management		

27	The solution should provide detail endpoint & authentication details		
28	The solution should provide role-based administrative access with dedicated roles for administrator, helpdesk operators etc.		
29	The solution should have http and SNI proxy based remediation options		
30	The solution should offer comprehensive visibility by automatically discovering, classifying, and controlling endpoints connected to the network to enable the appropriate services per endpoint of each & every device coming in to, getting out of and connected with the Bank 's network. Visibility must not only be limited to IP address, MAC address and Operating System but it should also include OS version, service running, process running, application version, application installed etc. to achieve 100% device visibility.		
31	Solution should support auto-remediation of PC clients as well as periodic reassessment to make sure the endpoint is not in violation of company policies and must check the end device compliance before permitting access to the network.		
32	Should have predefined device templates for a wide range of endpoints, such as IP phones, printers, IP cameras, smartphones, tablets and configurable templates. These templates can be used to automatically detect, classify, and associate administrative-defined identities when endpoints connect to the network. Administrators can also associate endpoint-specific authorization policies based on device type.		
33	Solution must support functionality in both managed and un-managed switches. Solution must help in uncovering of unmanaged & unknown Switches through number of hosts detection, etc. and block non-compliant endpoints which are connected to un-managed switches.		
34	Solution must be able to detect all users (domain as well as local) including local admin across all endpoints.		
35	Provides the ability to create powerful posture assessments policies by checking availability of latest OS patches, antivirus and antispysware software packages with current definition file variables (version, date, etc.), registries (key, value, etc.), and applications.		
36	The solution should support Bank 's existing network infrastructure i.e. managed & unmanaged switches to block or limit the non-complied and rogue devices behind that.		
37	The solution should enforce security policies by blocking, isolating, and repairing non-compliant machines in a quarantine area without requiring administrator attention.		
38	Solution must support auto-remediation on all the non- compliant end point like Update AV automatically, Update Patches automatically, Start Antivirus/ Patch Endpoint agent, Kill/ Uninstall blacklisted application/ Service/ process etc.		

39	Solution must detect and containment outbreak of known Virus/ Ransomware attacks based on custom IOC's shared by different regulatory body in different format like (CnC Address (Command and Control URL), Process (Process Name, Process Hash, Process Hash Type), File Exists (File Name, File Path), Mutex (Mutex Name), Registry Key (Path, Value), Service (Service name)).		
40	The proposed solution should be able to reflect immediate endpoint change, and automatically trigger configured host or network actions (e.g. user disables AV – automate immediate actions like notify user, force restart, etc.)		
41	Solution should have ability to generate reports in different formats, such as CSV/ PDF/ Excel, etc.		
42	The proposed solution should allow authorized administrator to, in case of emergency, bypass PC/Branch from the central manager/ management console.		
43	The Proposed solution should able to restrict communication to a non-compliant device which is connected to a hub/unmanaged switch, while another compliant device which should remain functional.		
44	The proposed solution should be able to provide complete software/application visibility for all windows endpoints i.e. all applications installed with exact version details, all processes running, all services running, etc.		
45	The proposed solution should support to monitor traffic from multiple segments simultaneously on a single appliance. Solution should have built in capabilities to add exceptions.		
46	The Solution should provide a powerful and flexible attribute-based access control that combines authentication, authorization, posture, profiling, and guest management services on a single platform.		
47	Solution must detect and containment outbreak of known Virus/ Ransomware attacks based on custom IOC's shared by different regulatory body in different format like (CnC Address (Command and Control URL), Process (Process Name, Process Hash, Process Hash Type), File Exists (File Name, File Path), Mutex (Mutex Name), Registry Key (Path, Value), Service (Service name)).		
48	Solution should be capable to detect the behaviour of state-change on endpoints after authenticating and authorizing. Like after granting the access has to monitor the endpoint for any state change with respect to compliance requirement.		
49	Must collect and keep forensic evidence on any unauthorized access activity within the network as follow: Event timestamp, network events in sequence, host info, IP address, MAC address, switch info, etc.		
50	OEM of the solution must have its own support presence in India		
51	The solution should integrate with VM infrastructure to provide out of the box visibility to Virtual Machine properties such as Boot Time, Virtual Machine Hardware, Virtual Machine is Orphan, Virtual Machine Peripheral Devices info, Virtual Machine Port Group, Virtual Machine Power State, Virtual Machine Usage CPU (one thousandth), Virtual Machine Usage Network I/O (KBps), etc.		

52	NAC solution must support out of box monitoring dashboard for all NAC server like CPU load , Device HDD , Device managed endpoints , Total Memory , Appliance traffic etc		
----	---	--	--

Sizing Document

#	Solutions	Sizing Parameter
1	Data Discovery & Classification	<ol style="list-style-type: none"> No. of File server - 3000 No. of databases - 100 No. of Users (Laptops / Desktops) - 39000
2	File Upload Security	<p>Sizing requirements for File Upload Security:</p> <ol style="list-style-type: none"> Number of web applications which is accepting files uploaded to it from internet/external network - 10 Number of web application protected by WAF which has files being uploaded - 15 Minimum & Maximum size of files uploaded to the application - 1KB to 250MB Number of concurrent files uploaded to the application (approx) during peak hours - 10 Number of files to uploaded to MFT at peak hours - 10 Minimum and Maximum size of files uploaded to MFT - 1KB to 250MB Number of sites (Eg. DC, DR,NDR etc.) which has WAF, MFT, Web applications - 2 (DC and DR)
3	Attack Surface Management (ASM)	<ol style="list-style-type: none"> No. of Assets - 1000 Digital Footprint - No. of URLs, domain, Public Ips - 1000

4	Breach and Attack Simulation (BAS)	<ol style="list-style-type: none"> 1. Number of Hosts in the environment - Endpoints + Server- 1000+5000 3. All attack vectors do they need, form the below list: <ol style="list-style-type: none"> a. Network Infiltration b. URL Filtering c. Endpoint - Windows, Linux, Mac (which one) d. Email Infiltration e. WAF f. Data Exfiltration 4. Existing OEMs for - <ol style="list-style-type: none"> a. 1. NGFW – Checkpoint, Cisco, Palo Alto, Fortinet b. 2. IPS – Cisco c. 3. WAF – F5, Citrix d. 4. SIEM – RSA NetWitness e. 5. EDR – TrendMicro
5	Phishing Simulation	<ol style="list-style-type: none"> 1. Number of users / employees - 20000 2. No. of Attack Vector of simulation <ol style="list-style-type: none"> a. Phishing, b. Ransomware, c. Vishing, d. Smsing, e. Whatsapp, f. QR Code, g. Attachment 3. Number of iteration (quarterly) - 3
6	AD Security	No. of Computer Systems - 45000

7	Governance, Risk and Compliance	<ul style="list-style-type: none"> • HA in DC and DRC • Module ITSM, Audit, Compliance, Business Continuity & 3rd party risk management. • Enterprise wide • Bank may further extend the quantity on similar rates • The licenses for all solutions should be perpetual in the name of — Central Bank of India. The OEMs should certify the same on their letterhead. • Total Number of users - 1000
8	Decoy (Honeytrap)	<ul style="list-style-type: none"> • Standalone in DC and Standalone in DR • 200 Vlan in DC, 200 Vlan in DR, 10 Vlan in DMZ in DC, 10Vlan in DMZ in DR • External threat intelligence decoy 5 • Bank may further extend the quantity to on similar rates during the contract tenure
9	Mobile Device Management	<p>2 at DC and 2 at DR</p> <ul style="list-style-type: none"> • Mobile Device Management - 7500 Devices - 7500 MDM License for mobile, laptop, tab etc - Mobile Threat Management - 7500 Devices - Additional 5500 MDM Licenses including Mobile Threat Management for tabs that are customized for Biometric authentication, Face recognition and print receipts. These tabs will be loaded with multiple apps as part of Digital Transformation • Bank may further extend the quantity to on similar rates during the tenure of the contract
10	Database Recovery and Ransomware Protection	The solution should be sized for the Database at 500 TB and should be expandable to 1PB.

RFP for Supply, Installation and Maintenance of
Cybersecurity Solutions and Associated
Hardware at the Bank

11	Network Access Control	<p>2 at DC and 2 at DR</p> <ul style="list-style-type: none"> • 45000 endpoints including desktops/ATMs/Kiosks • The licenses for all solutions should be perpetual in the name of —Central Bank of India. The OEMs should certify the same on their letterhead • Bank may further extend the quantity to on similar rates during the tenure of the contract
----	------------------------	---

56. Annexure 3: Conformity Letter

Date

To,

General Manager (IT),
Central Bank of India,
DIT, Sector 11,
CBD Belapur,
Navi Mumbai – 400614

Sir,

Sub: RFP for Supply, Installation and Maintenance of Cybersecurity Solutions and associated hardware at the Bank

Tender No. _____

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

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

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

Yours faithfully,

Authorized Signatory

Designation

Company Name

57. Annexure 4: Masked Commercial Bill of Material

Bidder to Masked Commercials in Annexure 1- Bill of Material and attached here

58. Annexure 5: Bidder's Information

#	Particulars	Details
1.	Name of bidder	
2.	Constitution	
3.	Address with Pin code	
4.	Authorized Person for bid	
5.	Contact Details (Mail id & Mob No)	
6.	Years of Incorporation	
7.	Number of years of experience in IT hardware items	
8.	Annual Turnover (In Rs.) 2021-22 – 2022-23 – 2023-24 –	
9.	Operating Profits (In Rs.) 2021-22 – 2022-23 – 2023-24 –	
10.	Net Worth (In Rs.) 2021-22 – 2022-23 – 2023-24 –	
11.	Whether OEM or authorized distributor	
12.	Number of service outlets across India	
13.	Good and Service Tax Number	
14.	Income Tax Number	
15.	Whether direct manufacturer or authorized dealers	
16.	Name and Address of OEMs	

17.	Brief Description of after sales service facilities available with the bidder.	
18.	Whether all RFP terms & conditions complied with.	

Signature

Name:

Designation:

Seal of Company

Date:

59. Annexure 6: Letter for Conformity of Product as per RFP

Date

To,

General Manager (IT),
Central Bank of India,
DIT, Sector 11,
CBD Belapur,
Navi Mumbai – 400614

Sir,

Sub: RFP for Supply, Installation and Maintenance of Cybersecurity Solutions and associated hardware at the Bank

Tender No. _____

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

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

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

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

Signature

Name:

Designation:

Seal of Company

Date:

60. Annexure 7: Undertaking for Acceptance of Terms of RFP

Date

To,

General Manager (IT),
Central Bank of India,
DIT, Sector 11,
CBD Belapur,
Navi Mumbai – 400614

Sir,

Sub: RFP for Supply, Installation and Maintenance of Cybersecurity Solutions and associated hardware at the Bank

Tender No. _____

With reference to RFP for Supply, Installation and Maintenance of Cybersecurity Solutions and associated hardware at the Bank:

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

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

Signature

Name:

Designation:

Seal of Company

Date:

61. Annexure 8: Manufacturer's Authorization Form

Date

To,

General Manager (IT),
Central Bank of India,
DIT, Sector 11,
CBD Belapur,
Navi Mumbai – 400614

Tender No. _____

Dear Sir,

We _____ (OEM Vendor) of _____ product / service / solution hereby authorize M/s. _____ (Selected Bidder / Vendor Name) to offer their quotation, negotiate and conclude the contract with you against the above invitation for the Bid. We hereby extend our full guarantee and comprehensive warranty and AMC & ATS (post expiry of warranty) as per terms and conditions of the tender and the contract for our product / application solution / services offered against this invitation for Bid by the above firm. We also extend our back-to-back service support and assurance of availability of our equipment (Hardware and Software as part of the Bill of Material) and their components as per terms and conditions of the tender, to M/s. _____ (Vendor Name) for a period of five years

Yours Faithfully,

Authorized Signatory

(Name, Phone No., Fax, E-mail)

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

62. Annexure 9: Integrity Pact

Integrity Pact

Between

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

And

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

Preamble

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

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

Section 1 – Commitments of the Principal

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

- a. No employee of the Principal, personally or through family members, will in connection with the tender for , or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.
- b. The Principal will, during the tender process treat all Bidder(s) with equity and reason. The Principal will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential / additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution.
- c. The Principal will exclude from the process all known prejudiced persons.

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

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

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

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

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

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

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

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

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

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

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

Section 4 – Compensation for Damages

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

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

Section 5 – Previous Transgression

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

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

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

- (1) The Bidder(s)/ Contractor(s) undertake(s) to demand from his subcontractors a commitment in conformity with this Integrity Pact.
- (2) The Principal will enter into agreements with identical conditions as this one with all Bidders and Contractors.
- (3) The Principal will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

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

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

Section 8 – Independent External Monitor / Monitors

- (1) The Principal appoints competent and credible Independent External Monitor for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.
- (2) The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. It will be obligatory for him to treat the information and documents of the Bidders/Contractors as confidential. He reports to the Chairman & Managing Director, CENTRAL BANK OF INDIA.
- (3) The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the Principal including that provided by the Contractor. The Contractor will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/ Contractor(s)/ Subcontractor(s) with confidentiality. In case of sub-contracting, the Principal Contractor shall take all responsibility of the adoption of Integrity Pact by the sub-contractor. In case of sub-contracting, the Principal Contractor shall take the responsibility of the adoption of the Integrity Pact by the sub-contractor.
- (4) The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Contractor. The parties offer to the Monitor the option to participate in such meetings.
- (5) As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit nonbinding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action. Parties to this agreement agree that they shall not approach the courts while representing the matter to IEM and will await IEM's decision in the matter. Parties to this agreement agree that they shall not approach the courts while representing the matter to IEM and will await IEM's decision in the matter.

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

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

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

Section 9 – Pact Duration

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

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

Section 10 – Other provisions

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

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

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

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

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

Section 11- FALL CLAUSE

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

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

63. Annexure 10: Non-Disclosure Agreement

This Agreement made at _____, on this ____ day of _____ 2024

Between

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

AND

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

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

WHEREAS:

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

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

1. Confidential Information

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

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

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

2. Non-Disclosure

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

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

3. Publications

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

4. Term

This Agreement shall be effective from the date hereof and shall continue till establishment of business relationship between the Parties and execution of definitive agreements thereafter. Upon expiration or termination as contemplated herein the Receiving Party shall immediately cease rights to any and all disclosures or uses of Confidential Information; and at the request of the Disclosing Party, the Receiving Party shall promptly return or destroy all written, graphic or other tangible forms of the Confidential Information and all copies, abstracts, extracts, samples, notes or modules thereof.

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

5. Title & Proprietary Rights

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

copy of the Confidential Information, and shall reproduce any such mark or notice on all copies of such Confidential Information. Likewise, the Receiving Party shall not add or emboss its own or any other any mark, symbol or logo on such Confidential Information.

6. Return of Confidential Information

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

7. Remedies

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

8. 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.

9. Governing Law and Jurisdiction

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

10. General

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

11. Indemnity

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

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

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

64. Annexure 11: Performance Bank Guarantee

To,
Central Bank of India
Mumbai

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

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

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

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

4) The Bank further undertakes not to revoke this Guarantee during its currency except with the previous consent of the purchaser in writing and this Guarantee shall continue to be enforceable till the aforesaid date of expiry or the last date of the extended period of expiry of Guarantee agreed upon by all the parties to this Guarantee, as the case may be, unless during the currency of this Guarantee all the dues of the purchaser under or by virtue of the said contract have been duly paid and its claims satisfied or discharged or the purchaser certifies that the terms and conditions of the said contract have been fully carried out by the contractor and accordingly discharges the Guarantee.

5) In order to give full effect to the Guarantee herein contained, you shall be entitled to act as if we are your principal debtors in respect of all your claims against the contractor hereby Guaranteed by

us as aforesaid and we hereby expressly waive all our rights of surety ship and other rights if any which are in any way inconsistent with the above or any other provisions of this Guarantee.

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

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

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

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

10) Notwithstanding anything contained herein:-

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

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

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

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

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

Date this ----- day of ----- 2024 at -----

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

sd/- -----

65. Annexure 12: Bid Security (Earnest Money Deposit)

To,

General Manager-IT
Central Bank of India,
DIT, 1st Floor,
CBD Belapur,
Navi Mumbai -400 614

Dear Sir,

In response to your invitation to respond to your RFP for Supply, Installation and Maintenance of Cybersecurity Solutions and associated hardware at the Bank, M/s _____ having their registered office at _____ (hereinafter called the "Bidder") wishes to respond to the said Request for Proposal (RFP) and submit the proposal for as listed in the RFP document.

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

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

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

Notwithstanding anything contained herein:

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

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

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

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

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

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

Yours faithfully,

For and on behalf of _____



RFP for Supply, Installation and Maintenance of
Cybersecurity Solutions and Associated
Hardware at the Bank

Bank Authorised Official

66. Annexure 13: Bidder's Particulars

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

Signature

Name:

Designation:

Seal of Company

Date:

67. Annexure 14: NPA Undertaking

Pro forma of letter to be given by all the bidders participating in RFP for Supply, Installation and Maintenance of Cybersecurity Solutions and associated hardware at the Bank on their official letter-head

Date:

To,
General Manager-IT,
Central Bank of India, Central Office,
Sector 11, CBD Belapur,
Navi Mumbai - 400614

Sir,

Sub: RFP for Supply, Installation and Maintenance of Cybersecurity Solutions and associated hardware at the Bank

Tender No. _____

We _____ (bidder name), hereby undertake that-

- We have not have been declared NPA by any Bank in India.
- Further, we do not have any pending case with any organization across the globe which affects our credibility to service the bank.

Yours faithfully,

Authorised Signatory

Designation

Bidder's corporate name

68. Annexure 15: Undertaking letter (Land Border Sharing)

Pro forma of letter to be given by all the bidders participating in RFP for the Supply, Installation and Maintenance of Cybersecurity Solutions and associated hardware at the Bank on their official letter-head

To

Date:

General Manager –IT,
Central Bank of India, Central Office,
Sector 11,
CBD Belapur,
Navi Mumbai – 400614

Sir,

Sub: RFP for Supply, Installation and Maintenance of Cybersecurity Solutions and associated hardware at the Bank

Tender No. _____

Dear Sir/Madam,

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

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

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

Strike off whichever is not applicable

1. "I/we have read the clause regarding restrictions on procurement from a bidder of the country which shares a land border with India; I/ we certify that _____ is not from such a country.
2. "I/we have read the clause regarding restrictions on procurement from a Bidder of a country which shares a land border with India; I/we certify that _____ is from such

a country. I hereby certify that _____ fulfils all requirements in this regard and is eligible to be considered. [Valid registration by the Competent Authority is attached]”

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

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

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

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

Dated this _____ by _____ 20__

Yours faithfully,

Authorized Signatory

Name:

Designation:

Bidder's Corporate Name:

Address:

Email & Phone No.:

List of documents enclosed:

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

Annexure 16: Cover Letter

Date:

To

General Manager-IT
DIT, Central Bank of India, Central Office,
Sector 11, CBD Belapur,
Mumbai - 400614

Sub: RFP for Supply, Installation and Maintenance of Cybersecurity Solutions and associated hardware
at the Bank

Tender No. _____

Dear Sir/Madam,

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

Authorised Signatory

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

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

69. Annexure 17: Pre-bid Query Format

Queries:

Sr. No.	Page #	Point / Section #	Query	Banks Response (Bidder Should not fill in this column)
1				
2				
3				
4				
5				
6				
7				
8				
9				

Date:

Authorised Signatory & Stamp

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

70. Annexure 18: Eligibility Criteria Compliance

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

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

The Bidder must fulfil following eligibility criteria

#	Eligibility of the Bidder	Documents to be submitted	Compliance (Y/N)
1.	Bidder should be a Registered company under Indian Companies Act. 1956/2013 or LLP/Partnership firm and should have been in existence for a minimum period of 5 years in India, as on date of submission of RFP.	Copy of the Certificate of Incorporation issued by Registrar of Companies/Registrar of firms and full address of the registered office of the bidder	
2.	Bidder should be registered under G.S.T and/or tax registration in state where bidder has a registered office	Proof of registration with GSTIN	
3.	The bidder must have an average annual turnover in India of INR 500 crores per annum in the last three financial years (i.e., 2021-22, 2022-23, 2023-24) at the time of submission of tender, of individual company and not as group of companies*	Copy of Audited Balance Sheet and Copy of Certificate of the Chartered Accountant for the last three financial years (i.e., 2021-22, 2022-23, 2023-24)	
4.	The bidder should have made operating profits in at least two financial years out of last three financial years (i.e., 2021-22, 2022-23, 2023-24)* In case of operating loss, bidder will have to provide additional security amount of 20% of contract Value over and above 10% of regular Performance Bank Guarantee	Copy of Audited Balance Sheet and Copy of Certificate of the Chartered Accountant for the last three financial years (i.e., 2021-22, 2022-23, 2023-24)	
5.	The bidder should have a positive net worth in last three financial years (i.e., 2021-22, 2022-23, 2023-24)*	Copy of Audited Balance Sheet and Copy of Certificate of the Chartered Accountant for the last three financial	

#	Eligibility of the Bidder	Documents to be submitted	Compliance (Y/N)
		years (i.e., 2021-22, 2022-23, 2023-24)	
6.	At the time of bidding, the Bidder should not have been blacklisted/debarred/ by any Govt. / IBA/RBI/PSU /PSE/ or Banks, Financial institutes for any reason or non-implementation/ delivery of the order. Self-declaration to that effect should be submitted along with the technical bid.	Submit the undertaking on Company's letter head	
7.	At the time of bidding, there should not have been any pending litigation or any legal dispute in the last five years, before any court of law between the Bidder or OEM and the Bank regarding supply of goods/services	Submit the undertaking self-declaration on Company's letter head	
8.	Bidder/OEM should not have <ul style="list-style-type: none"> NPA with any Bank /financial institutions in India Any case pending or otherwise, with any organization across the globe which affects the credibility of the Bidder in the opinion of Central Bank of India to service the needs of the Bank 	Submit self-declaration on Company's letter head.	
9.	Bidder should have service/support centre or should have arrangement for providing support in Mumbai and Hyderabad.	Submit the undertaking self-declaration on Bidder's letter head	
10.	If the bidder is from a country which shares a land border with India, the bidder should be registered with the Competent Authority	Certified copy of the registration certificate	
11.	Bidder should have a supplied, installed and maintained at least 4 out of the following solutions: <ol style="list-style-type: none"> Data Discovery & Classification File Upload Security Solution Attack Surface Management (ASM) Breach and Attack Simulation (BAS) along with Red Team Solution Phishing Simulation AD Security IT Governance, Risk & Compliance Decoy (Honey-pot) Mobile Device Management 	Reference Letter/ Purchase order of similar projects undertaken.	

#	Eligibility of the Bidder	Documents to be submitted	Compliance (Y/N)
	<p>10. Secure Data Backup and Recovery (Ransomware Protection)</p> <p>11. Network Access Control (NAC)</p> <p>in at least One Scheduled Commercial Banks/ "Govt/Public" Listed BFSI/ RBI/ NABARD/ NPCI in India.</p>		
OEM Eligibility Criteria			
12.	<p>For the proposed OEMs' solutions product series, minimum 7 out of the below solutions must have been implemented in at least One Scheduled Commercial Bank/ "Govt/Public" Listed BFSI/ RBI/ NABARD/ NPCI in India in last 5 years.</p> <ol style="list-style-type: none"> 1. Data Discovery & Classification 2. File Upload Security Solution 3. Attack Surface Management (ASM) 4. Breach and Attack Simulation (BAS) along with Red Team Solution 5. Phishing Simulation 6. AD Security 7. IT Governance, Risk & Compliance 8. Decoy (HoneyPot) 9. Mobile Device Management 10. Secure Data Backup and Recovery (Ransomware Protection) 11. Network Access Control (NAC) 	Reference Letter/ Purchase order of similar projects undertaken.	

***Note:** If case of unaudited Balance Sheet for FY 2023-24, Bidder needs to submit Provisional Balance Sheet along with copy of CA Certificate for FY 2023-24

Authorised Signatory

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

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

71. Annexure 19: Guidelines on banning of business dealing GUIDELINES FOR INDIAN AGENTS OF FOREIGN SUPPLIERS

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

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

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

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

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

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

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

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

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

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

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

2.2.3 Confirmation of the foreign principals of the Tenderer that the commission/remuneration, if any, reserved for the Tenderer in the quoted price (s), may be paid by CENTRAL BANK OF INDIA in India in equivalent Indian Rupees on satisfactory completion of the Project or supplies of Stores and Spares in case of operation items .

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

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

Sr. Contents

1. Introduction
2. Scope
3. Definitions
4. Initiation of banning / suspension
5. Suspension of business dealing
6. Ground on which banning of business dealings can be initiated
7. Banning of business dealings
8. Removal from list of approved agencies –suppliers/contractors
9. Show-cause notice
10. Appeal against the competent authority
11. Review of the decision by the competent authority
12. Circulation of names of agencies with whom business dealings have been banned

1. Introduction

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

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

2. Scope

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

provide that CENTRAL BANK OF INDIA reserves its rights to remove from list of approved suppliers / contractors or to ban business dealings if any Agency has been found to have committed misconduct

and also to suspend business dealings pending investigation. If such provision does not exist in any GCC, the same may be incorporated.

2.2 Similarly, in case of sale of material there is a clause to deal with the Agencies / customers

/ Buyers, who indulge in lifting of material in unauthorized manner. If such a stipulation does not exist in any Sale Order, the same may be incorporated.

2.3 However, absence of such a clause does not in any way restrict the right of Bank (CENTRAL BANK OF INDIA) to take action / decision under these guidelines in appropriate cases.

2.4 The procedure of (i) Removal of Agency from the List of approved suppliers / contractors; (ii) Suspension and (iii) Banning of Business Dealing with Agencies, has been laid down in these guidelines.

2.5 These guidelines apply to all the Units and subsidiaries of CENTRAL BANK OF INDIA.

2.6 It is clarified that these guidelines do not deal with the decision of the Management not to entertain any particular Agency due to its poor / inadequate performance or for any other reason.

2.7 The banning shall be with prospective effect, i.e., future business dealings.

3. Definitions

In these Guidelines, unless the context otherwise requires:

- i) 'Party / Contractor / Supplier / Purchaser / Customer/Bidder/Tenderer' shall mean and include a public limited Bank or a private limited Bank, a firm whether registered or not, an individual, a cooperative society or an association or a group of persons engaged in any commerce, trade, industry, etc. 'Party / Contractor / Supplier / Purchaser / Customer/ Bidder / Tenderer' in the context of these guidelines is indicated as 'Agency'.
- ii) 'Inter-connected Agency' shall mean two or more companies having any of the following features:
 - a) If one is a subsidiary of the other.
 - b) If the Director(s), Partner(s), Manager(s) or Representative(s) are common;
 - c) If management is common;
 - d) If one owns or controls the other in any manner;
- iii) 'Competent Authority' and 'Appellate Authority' shall mean the following:
 - a) For Bank (entire CENTRAL BANK OF INDIA) wide Banning Executive Director (BSD) shall be the "Competent Authority" for the purpose of these guidelines. Chairman & Managing Director, CENTRAL BANK OF INDIA shall be the "Appellate Authority" in respect of such cases except banning of business dealings with Foreign Suppliers of imported coal/coke.
 - b) For banning of business dealings with Foreign Suppliers of imported goods, CENTRAL BANK OF INDIA Executive Directors" Committee (EDC) shall be the "Competent Authority". The Appeal against the Order passed by EDC, shall lie with Chairman & Managing Director, as First Appellate Authority.
 - c) In case the foreign supplier is not satisfied by the decision of the First Appellate Authority, it may approach CENTRAL BANK OF INDIA Board as Second Appellate Authority.

d) For Zonal Offices Only

Any officer not below the rank of Deputy General Manager appointed or nominated by the Head of Zonal Office shall be the "Competent Authority" for the purpose of these guidelines. The Head of the concerned Zonal Office shall be the "Appellate Authority" in all such cases. e) For Corporate Office only

For procurement of items / award of contracts, to meet the requirement of Corporate Office only, Head of Business Support Department (BSD) shall be the "Competent Authority" and concerned Executive Director (BSD) shall be the "Appellate Authority".

e) Managing Director & CEO, CENTRAL BANK OF INDIA shall have overall power to take suo-moto action on any information available or received by him and pass such order(s) as he may think appropriate, including modifying the order(s) passed by any authority under these guidelines.

iv) 'Investigating Department' shall mean any Department or Unit investigating into the conduct of the Agency and shall include the Vigilance Department, Central Bureau of Investigation, the State Police or any other department set up by the Central or State Government having powers to investigate.

v) 'List of approved Agencies - Parties / Contractors / Suppliers / Purchasers / Customers / Bidders / Tenderers shall mean and include list of approved / registered Agencies - Parties/ Contractors / Suppliers / Purchasers / Customers / Bidders / Tenderers, etc.

4. Initiation of Banning / Suspension

Action for banning / suspension business dealings with any Agency should be initiated by the department having business dealings with them after noticing the irregularities or misconduct on their part. Besides the concerned department, Vigilance Department of each Unit /Corporate Vigilance may also be competent to advise such action.

5. Suspension of Business Dealings

5.1 If the conduct of any Agency dealing with CENTRAL BANK OF INDIA is under investigation by any department (except Foreign Suppliers of imported goods), the Competent Authority may consider whether the allegations under investigation are of a serious nature and whether pending investigation, it would be advisable to continue business dealing with the Agency. If the Competent Authority, after consideration of the matter including the recommendation of the Investigating Department, if any, decides that it would not be in the interest to continue business dealings pending investigation, it may suspend business dealings with the Agency. The order to this effect may indicate a brief of the charges under investigation. If it is decided that inter-connected Agencies would also come within the ambit of the order of suspension, the same should be specifically stated in the order. The order of suspension would operate for a period not more than six months and may be communicated to the Agency as also to the Investigating Department. The Investigating Department may ensure that their investigation is completed and whole process of final order is over within such period.

5.2 The order of suspension shall be communicated to all Departmental Heads within the Plants / Units. During the period of suspension, no business dealing may be held with the Agency.

5.3 As far as possible, the existing contract(s) with the Agency may continue unless the Competent Authority, having regard to the circumstances of the case, decides otherwise.

5.4 If the gravity of the misconduct under investigation is very serious and it would not be in the interest of CENTRAL BANK OF INDIA, as a whole, to deal with such an Agency pending investigation, the Competent Authority may send his recommendation to ED (GAD), CENTRAL BANK OF INDIA Corporate Office along with the material available. If Corporate Office considers that depending upon the gravity of the misconduct, it would not be desirable for all the Units and Subsidiaries of CENTRAL BANK OF INDIA to have any dealings with the Agency concerned, an order suspending business dealings may be issued to all the Units by the Competent Authority of the Corporate Office, copy of which may be endorsed to the Agency concerned. Such an order would operate for a period of six months from the date of issue.

5.5 For suspension of business dealings with Foreign Suppliers of imported goods, following shall be the procedure:-

i) Suspension of the foreign suppliers shall apply throughout the Bank including Subsidiaries. ii) Based on the complaint forwarded by ED (BSD) or received directly by Corporate Vigilance, if gravity of the misconduct under investigation is found serious and it is felt that it would not be in the interest of CENTRAL BANK OF INDIA to continue to deal with such agency, pending investigation, Corporate Vigilance may send such recommendation on the matter to Executive Director, BSD to place it before Executive Directors Committee (EDC) with ED (BSD) as Convener of the Committee. The committee shall expeditiously examine the report, give its comments/recommendations within twenty one days of receipt of the reference by ED, BSD.

iii) If EDC opines that it is a fit case for suspension, EDC may pass necessary orders which shall be communicated to the foreign supplier by ED, BSD.

5.6 If the Agency concerned asks for detailed reasons of suspension, the Agency may be informed that its conduct is under investigation. It is not necessary to enter into correspondence or argument with the Agency at this stage.

5.7 It is not necessary to give any show-cause notice or personal hearing to the Agency before issuing the order of suspension. However, if investigations are not complete in six months' time, the Competent Authority may extend the period of suspension by another three months, during which period the investigations must be completed.

6. Ground on which Banning of Business Dealings can be initiated

6.1 If the security consideration, including questions of loyalty of the Agency to the State, so warrant;

6.2 If the Director / Owner of the Agency, proprietor or partner of the firm, is convicted by a Court of Law for offences involving moral turpitude in relation to its business dealings with the Government or any other public sector enterprises or CENTRAL BANK OF INDIA, during the last five years;

6.3 If there is strong justification for believing that the Directors, Proprietors, Partners, owner of the Agency have been guilty of malpractices such as bribery, corruption, fraud, substitution of tenders, interpolations, etc.;

6.4 If the Agency continuously refuses to return / refund the dues of CENTRAL BANK OF INDIA without showing adequate reason and this is not due to any reasonable dispute which would attract proceedings in arbitration or Court of Law;

6.5 If the Agency employs a public servant dismissed / removed or employs a person convicted for an offence involving corruption or abetment of such offence;

6.6 If business dealings with the Agency have been banned by the Govt. or any other public sector enterprise;

6.7 If the Agency has resorted to Corrupt, fraudulent practices including misrepresentation of facts and / or fudging /forging /tampering of documents;

6.8 If the Agency uses intimidation / threatening or brings undue outside pressure on the Bank (CENTRAL BANK OF INDIA) or its official in acceptance / performances of the job under the contract;

6.9 If the Agency indulges in repeated and / or deliberate use of delay tactics in complying with contractual stipulations;

6.10 Wilful indulgence by the Agency in supplying sub-standard material irrespective of whether pre-dispatch inspection was carried out by Bank (CENTRAL BANK OF INDIA) or not;

6.11 Based on the findings of the investigation report of CBI / Police against the Agency for malafide / unlawful acts or improper conduct on his part in matters relating to the Bank

(CENTRAL BANK OF INDIA) or even otherwise;

6.12 Established litigant nature of the Agency to derive undue benefit;

6.13 Continued poor performance of the Agency in several contracts;

6.14 If the Agency misuses the premises or facilities of the Bank (CENTRAL BANK OF INDIA), forcefully occupies, tampers or damages the Bank's properties including land, water resources, forests / trees, etc.

(Note: The examples given above are only illustrative and not exhaustive. The Competent Authority may decide to ban business dealing for any good and sufficient reason).

7 Banning of Business Dealings

7.1 A decision to ban business dealings with any Agency should apply throughout the Bank Including Subsidiaries.

7.2 There will be a Standing Committee in each Zone to be appointed by Head of Zonal Office for processing the cases of "Banning of Business Dealings" except for banning of business dealings with foreign suppliers of goods. However, for procurement of items / award of contracts, to meet the requirement of Corporate Office only, the committee shall be consisting of General Manager / Dy. General Manager each from Operations, Law & BSD. Member from BSD shall be the convener of the committee. The functions of the committee shall, inter-alia include:

i) To study the report of the Investigating Agency and decide if a prima-facie case for Bank- wide / Local unit wise banning exists, if not, send back the case to the Competent Authority. ii) To recommend for issue of show-cause notice to the Agency by the concerned department. iii) To examine the reply to show-cause notice and call the Agency for personal hearing, if required.

iv) To submit final recommendation to the Competent Authority for banning or otherwise.

7.3 If Bank wide banning is contemplated by the banning Committee of any Zone, the proposal should be sent by the committee to ED (BSD) through the Head of the Zonal Office setting out the facts of the case and the justification of the action proposed along with all the relevant papers and documents. GAD shall get feedback about that agency from all other Zones and based on this feedback, a prima-facie decision for banning / or otherwise shall be taken by the Competent Authority. At this stage if it is felt by the Competent Authority that there is no sufficient ground for Bank wide banning, then the case shall be sent back to the Head of Zonal Office for further action at the Zone level. If the prima-facie decision for Bank-wide banning has been taken, ED (BSD) shall issue a show-cause notice to the agency conveying why it should not be banned throughout CENTRAL BANK OF INDIA.

After considering the reply of the Agency and other circumstances and facts of the case, ED (BSD) will submit the case to the Competent Authority to take a final decision for Bank-wide banning or otherwise.

7.4 If the Competent Authority is prima-facie of view that action for banning business dealings with the Agency is called for, a show-cause notice may be issued to the Agency as per paragraph 9.1 and an enquiry held accordingly.

7.5 Procedure for Banning of Business Dealings with Foreign Suppliers of imported goods.

- Banning of the agencies shall apply throughout the Bank including Subsidiaries.
- Based on the complaint forwarded by ED (BSD) or received directly by Corporate Vigilance, if gravity of the misconduct under investigation is found serious and it is felt that it would not be in the interest of CENTRAL BANK OF INDIA to continue to deal with such agency, pending investigation, Corporate Vigilance may send such recommendation on the matter to Executive Director, BSD to place it before Executive Directors[^] Committee (EDC) with ED (BSD) as Convener of the Committee.
- The committee shall expeditiously examine the report, give its comments/recommendations within twenty one days of receipt of the reference by ED, BSD.
- If EDC opines that it is a fit case for initiating banning action, it will direct ED (BSD) to issue show-cause notice to the agency for replying within a reasonable period.
- On receipt of the reply or on expiry of the stipulated period, the case shall be submitted by ED (BSD) to EDC for consideration & decision.
- The decision of the EDC shall be communicated to the agency by ED (BSD).

8 Removal from List of Approved Agencies - Suppliers / Contractors, etc.

8.1 If the Competent Authority decides that the charge against the Agency is of a minor nature, it may issue a show-cause notice as to why the name of the Agency should not be removed from the list of approved Agencies - Suppliers / Contractors, etc.

8.2 The effect of such an order would be that the Agency would not be disqualified from Competing in Open Tender Enquiries but Limited Tender Enquiry (LTE) may not be given to the Agency concerned.

8.3 Past performance of the Agency may be taken into account while processing for approval of the Competent Authority for awarding the contract.

9 Show Cause Notice

9.1 In case where the Competent Authority decides that action against an Agency is called for, a show-cause notice has to be issued to the Agency. Statement containing the imputation of misconduct or misbehaviour may be appended to the show-cause notice and the Agency should be asked to submit within 15 days a written statement in its defense.

9.2 If the Agency requests for inspection of any relevant document in possession of CENTRAL BANK OF INDIA, necessary facility for inspection of documents may be provided.

9.3 The Competent Authority may consider and pass an appropriate speaking order:

- a) For exonerating the Agency if the charges are not established;
- b) For removing the Agency from the list of approved Suppliers / Contactors, etc. c) For banning the business dealing with the Agency.

9.4 If it decides to ban business dealings, the period for which the ban would be operative may be mentioned. The order may also mention that the ban would extend to the interconnected Agencies of the Agency.

10 Appeal against the Decision of the Competent Authority

10.1 The Agency may file an appeal against the order of the Competent Authority banning business dealing, etc. The appeal shall lie to Appellate Authority. Such an appeal shall be preferred within one month from the date of receipt of the order banning business dealing, etc.

10.2 Appellate Authority would consider the appeal and pass appropriate order which shall be communicated to the Agency as well as the Competent Authority.

11 Review of the Decision by the Competent Authority

Any petition / application filed by the Agency concerning the review of the banning order passed originally by Competent Authority under the existing guidelines either before or after filing of appeal before the Appellate Authority or after disposal of appeal by the Appellate Authority, the review petition can be decided by the Competent Authority upon disclosure of new facts / circumstances or subsequent development necessitating such review. The Competent Authority may refer the same petition to the Standing Committee/EDC as the case may be for examination and recommendation.

12 Circulation of the names of Agencies with whom Business Dealings have been banned

12.1 Depending upon the gravity of misconduct established, the Competent Authority of the Corporate Office may circulate the names of Agency with whom business dealings have been banned, to the Government Departments, other Public Sector Enterprises, etc. for such action as they deem appropriate.

12.2 If Government Departments or a Public Sector Enterprise request for more information about the Agency with whom business dealings have been banned, a copy of the report of Inquiring

Authority together with a copy of the order of the Competent Authority / Appellate Authority may be supplied.

12.3 If business dealings with any Agency has been banned by the Central or State Government or any other Public Sector Enterprise, CENTRAL BANK OF INDIA may, without any further enquiry or investigation, issue an order banning business dealing with the Agency and its inter-connected Agencies.

12.4 Based on the above, Zonal Offices may formulate their own procedure for implementation of the Guidelines and same be made a part of the tender documents



72. Annexure 20: Compliance Certificate with respect to RBI's "Master Direction on Outsourcing of Information Technology Services"

(This letter should be on the letterhead of the bidder)

Date: _____

To,
General Manager-IT
DIT, Central Bank of India, Central Office,
Sector 11, CBD Belapur,
Mumbai – 400614

Subject: RFP - _____ - Compliance Certificate with respect to Chapter II para 4c of RBI's "Master Direction on Outsourcing of Information Technology Services"

Sir,

With reference to above, we <<<<Name of the Company>>>> hereby furnish and confirm the details as given below: -

1. Date of Agreement-
2. Expiry Date of Agreement
3. Type of Entity: Group Company/Not a group Company
4. Name of Directors of Company
5. Is any of the Director(s), Key Managerial Personnel and their relatives are stated above related to Central Bank of India: YES/NO

Note: - The terms 'control', 'director', 'key managerial personnel', and 'relative' have the same meaning as assigned under the Companies Act, 2013 and the Rules framed thereunder from time to time.

Authorized Signatory Name:

Designation:

Email and Phone