



Central Bank of India

Tender Reference Number: CO:DIT:PUR:2017-18:252

Request for Proposal

For

Supply, Installation and Maintenance of Security Solutions

Dated: 31 October 2017

Contents

List of Annexure:	8
List of Appendix:	8
Purpose of the Document	9
Definitions and Acronyms	9
1. Introduction	11
1.1 Invitation for Tender Offer	11
1.2 About the Bank	11
1.3 Project Objective	12
1.4 Project Scope	12
1.5 Project Timelines	13
1.6 Schedule of Events.....	16
1.7 Pre Bid Meeting	17
2. Detailed Scope of Work	18
2.1 General	18
2.1.1 Functional Principles.....	18
2.1.2 Scalability Principles	18
2.1.3 Availability Principles	18
2.1.4 Performance Principles.....	18
2.2 Scope of Work for Each Security Solutions	19
2.2.1 Advance Threat prevention.....	19
2.2.2 Host Intrusion Prevention Detection (HIPS).....	21
2.2.3 Application Change Control	22
2.2.4 Mobile Device Management	24
2.2.5 Distributed Denial of Service (DDoS).....	25
2.2.6 Network Access Control.....	25
2.2.7 Digital Rights Management.....	28
2.2.8 Endpoint Encryption.....	29
2.2.9 IT Security Governance Risk and Compliance	31

2.2.10	Brand Protection	32
2.2.11	Decoy (Honey Pot)	33
2.2.12	API Management	34
2.2.13	Application Security Testing.....	35
2.2.14	Vulnerability Management	36
2.2.15	Firewall Analyzer	37
2.2.16	Data Loss Prevention	38
2.3	General Responsibility of the Bidders and OEM	41
2.3.1	Training.....	44
2.3.2	Implementation & Integration	45
2.3.3	Continuous Improvement.....	46
2.3.4	Solution Acceptance	46
2.3.5	System Integration Testing (SIT) and User Acceptance Testing (UAT)	46
2.3.6	Workflow Automation.....	47
2.3.7	SLA compliance.....	47
2.3.8	Business Continuity	47
2.4	Service Level Agreements.....	47
2.4.1	service levels during implementation phase	47
2.4.2	Monitoring and Operations.....	48
2.4.3	Penalty.....	53
2.4.4	Responsibility Matrix.....	54
2.4.5	Tables of Incident Matrix.....	54
3.	Terms and Conditions	54
3.1	General	55
3.1.1	Two Bid System.....	55
3.1.2	Date of Submission.....	57
3.1.3	Liabilities of Bank.....	57
3.1.4	Proposal Process Management.....	57

3.1.5	Date of Bid Expiration	57
3.1.6	Bidder Indication of Authorization to Bid	57
3.1.7	RFP Ownership	58
3.1.8	Proposal Ownership	58
3.1.9	Bid Pricing Information.....	58
3.1.10	Bidder Status	58
3.1.11	Confidentiality	58
3.1.12	Disclaimer	60
3.1.13	Right to Reject	61
3.1.14	Bid Security.....	61
3.2	Terms of Reference (TOR)	61
3.2.1	Ownerships, Grant and Delivery	61
3.2.2	Acceptance Testing	62
3.2.3	Compliance with Laws	63
3.2.4	Assignment	63
3.2.5	Insurance	64
3.2.6	Order Cancellation	65
3.2.7	Indemnity	65
3.2.8	Publicity	66
3.2.9	Solicitation of Employees.....	66
3.2.10	Information Ownership.....	67
3.2.11	Confidentiality	67
3.2.12	Technological Advancements	69
3.2.13	Successful Bidder's Liability.....	70
3.2.14	Guarantees	70
3.2.15	Force Majeure.....	70
3.2.16	Resolution of Disputes and remedies	71
3.2.17	Exit Option and Contract Re-Negotiation	72

3.2.18	Severability	72
3.2.19	Corrupt and Fraudulent Practices	73
3.2.20	Waiver.....	73
3.2.21	Violation of Terms.....	73
3.2.22	Termination.....	74
3.2.23	Effect of Termination.....	75
3.2.24	Format for Technical Offer	75
3.2.25	Other General Conditions	76
3.2.26	Costs & Currency Price Composition.....	77
3.2.27	Fixed Price	78
3.2.28	Project Completion Time.....	78
3.2.29	Completeness of Installation.....	78
3.2.30	Liquidated Damages	79
3.2.31	Blacklisting	79
3.2.32	Hardware Warranty.....	79
3.2.33	Annual Maintenance Charges.....	80
3.2.34	Facility Management.....	81
3.2.35	Performance Bank Guarantee	81
3.2.36	Non-Disclosure Agreement.....	82
3.2.37	Cancellation of Order	82
3.2.38	Security	82
3.2.39	Patent Rights/ Intellectual Property Rights.....	82
3.2.40	Audit/ Review/Monitoring/Visitation.....	83
3.2.41	Independent Contractor	84
3.2.42	Amendments.....	85
3.2.43	Counterparts	85
3.2.44	Governing Law and Jurisdiction	85
3.2.45	Change Control Process.....	85

3.2.46	Acceptance of Terms & Conditions.....	85
3.2.47	No liability of the Bank towards employees/ agents of successful Bidder	85
4.	Eligibility Criteria.....	86
4.1.1	Eligibility Criteria for Bidder.....	86
5.	Project Team Structure.....	90
5.1	Project Implementation Phase	90
5.1.1	Roles and Responsibilities.....	90
5.1.2	Comprehensive project management services	90
5.1.3	Implementation Project Manager	91
5.1.4	Team Lead for respective Solutions	91
5.1.5	Implementation Team	91
5.1.6	OEM Team	91
5.2	Operation Phase	92
6.	Bidder Evaluation & Methodology.....	93
6.1	Normalization of bids	93
6.2	General Eligibility Criteria	93
6.3	Technical Evaluation.....	94
6.4	Commercial Evaluation.....	95
6.4.1	Reverse Auction	96
6.4.2	Commercial Bid Evaluation Considerations	96
7.	Payment Terms	98
7.1	Procedure for claiming payments	98
7.2	Product Cost	98
7.3	AMC & ATS and other Warranty Costs.....	99
8.	Definitions & Reference.....	103
8.1	Working Day	103
8.2	Business Hours.....	103
8.3	Restore to Service.....	103
8.3.1	Obligation of the Bidder	103
8.4	Obligation of the Bank.....	104

9. Disclaimer..... 105

LIST OF ANNEXURE:

Annexure 1 – Conformity Letter
 Annexure 2 – Conformity with Hardcopy Letter
 Annexure 3 – Bidder Capability Criteria Questionnaire
 Annexure 4 – Eligibility Criteria Compliance
 Annexure 5 – List of Branches
 Annexure 6 – Service Centre Details
 Annexure 7 – Minimum technical specification
 Annexure 8 – Reverse Auction Procurement Procedure
 Annexure 9 – Indicative Commercial Bid – Bill of Materials
 Annexure 10 – Reference Site Details
 Annexure 11 – Sizing Requirement
 Annexure 12 – Payment Terms
 Annexure 13 – Integrity – Pact

LIST OF APPENDIX:

Appendix 1 Form B 01 – Bill of Materials
 Appendix 2 Form A 01 – Cover TO
 Appendix 2 Form A 02 – Query on T&C
 Appendix 2 Form A 03 – Query Format
 Appendix 2 Form A 04 – Manufacturer Authorization
 Appendix 2 Form A 05 – Bid Security Form
 Appendix 2 Form A 06 – Performance Bank Guarantee
 Appendix 2 Form A 07 – Non-Disclosure Agreement
 Appendix 2 Form A 08 – Letter from OEMs

PURPOSE OF THE DOCUMENT

The Request for Proposal (hereafter referred to as “RFP”) document is meant to define the scope of work to the Bidder for “Supply, Implementation and Maintenance of security solutions” at Central Bank of India as per the terms, conditions and specifications provided in the RFP.

This RFP contains the details regarding scope, project timelines, evaluation process, terms and conditions as well as other relevant details which Bidder needs to factor while responding to this RFP. The objective of this RFP is to find a suitable Bidder, who can deliver the in scope solutions in alignment to the requirements of Central Bank of India, hereafter called as “Bank”, but also to have proven experience in the area of IT security for banking sector to respond to this RFP.

Note: This RFP should not be considered as a statement of intent for procurement, unless a purchase order or notification of award is published by Bank if any, as an end result of this RFP process.

DEFINITIONS AND ACRONYMS

Following terms are used in the document interchangeably to mean:

“API” – Application Programming Interface
“ATP” – Advanced Threat Prevention
“ATS” – Annual Technical Support
“ACC” – Application Change Control
“Bank” means ‘Central Bank of India’
“CBS” - Core Banking Solution
“CO” - Central Office
“CPU” - Central Processing Unit
“CVC” - Central Vigilance Commission
“DC” - Data Centre of the Bank, which is located at Data Centre Office, Belapur, Mumbai
“DDoS” – Distributed Denial of Service
“DMZ” - Demilitarized Zone
“DRC” - Disaster Recovery Centre, which is located in Hyderabad
“DRM” – Digital Rights Management
“Equipment” – Hardware and Software
“GM - IT” - General Manager – Information Technology
“HO” - Head Office
“INR” - Indian National Rupee
“HIPS” - Intrusion Prevention System
“IT” - Information Technology
“LAN” - Local Area Network
“Mbps” - Million bits Per Second
“MDM” – Mobile Device Management
“MPPS” - Million Packets per Second
“MTBF” - Mean Time before Failure
“NAC” – Network Access Control
“PO” - Purchase Order
“OEM” - Original Equipment Manufacturer
Bank shall be individually referred to as ‘Party’ and collectively as ‘Parties’
“RFP” - Request for Proposal “RO” - Regional Office
“SMTP” - Simple Mail Transfer Protocol

“SI” - System Integrator
“SoW” - Scope of Work
“T&C” - Terms & Conditions
“TCO” - Total Cost of Ownership
“TCP” - Transmission Control Protocol
“ToR” - Terms of Reference
“TPS” - Transactions per Second
“UAT” - User Acceptance Test
“VM” – Vulnerability Management
“WAF” – Web Application Firewall
“WAN” - Wide Area Network
“ZO” - Zonal Office

“BIDDER” - Single point appointed by the Bank for procurement, supply, implement and maintain of the equipment, based the bill of materials shared by the Bank.

1. INTRODUCTION

1.1 INVITATION FOR TENDER OFFER

Central Bank of India (hereby referred to as “Bank”) invites sealed tenders for Technical bid and Commercial bid from suitable and experienced IT service providers for Supply, Installation, Implementation, Integration and Maintenance of Security Solutions mentioned in this RFP. Bidder refers to the bidder delivering products / services mentioned in this RFP.

The prospective bidders are advised to note the following:

- The Bank expects the interested Bidders to purchase the hardcopy/softcopy of the complete RFP document including complete set of annexures and appendices from the Bank’s premises during the business hours as per schedule. The interested bidders are required to submit the Non-refundable Tender Document Fees of Rs.5,000/- (Rupees Five Thousand only) by way of demand draft from any Scheduled Commercial Bank in favor of ‘Central Bank of India’ payable at Mumbai to receive the RFP document. The RFP document without the set of annexures and appendices can be downloaded from the Bank’s website.
- Bidders, who have purchased Tender document Fees of Rs.5,000/- (Rupees Five Thousand) by way of Demand Draft from any Scheduled Commercial Bank in favor of “Central Bank of India” payable at Mumbai, are only allowed to attend the pre-bid meeting. If any Bidder chose not to attend the pre-bid meeting, their queries if any may not be entertained by the Bank, However, they can participate in the RFP process.
- Bank will respond to queries of bidders who have purchased tender document. Representatives of bidders are required to carry an authorization document from the company, an identity card for attending the pre-bid meeting. Only two representative of Bidders can attend the pre-bid meeting.
- Bidders are required to submit Bank guarantee/Demand Draft in favor of “Central Bank of India” payable at Mumbai, towards Earnest money Deposit (EMD) for Rs.2,00,00,000/- (Rupees Two Crore only). The Bank may accept Bank guarantee in lieu of Demand draft for an equivalent amount valid for 210 days issued by any Scheduled Commercial Bank acceptable to the Bank. Offers made without EMD will be rejected.
- Technical Specifications, Bill of Material documents, Terms and Conditions and various formats for submitting the tender offer are described in the tender document and Annexures.

1.2 ABOUT THE BANK

Central Bank of India herein after referred to as the “Bank”, established in 1911, was nationalized in the year 1969 and today is a leading public sector Bank listed in BSE/NSE.

The organizational structure of the Bank consists of four tiers viz., Central Office (CO), Zonal Offices (ZO) and Branches. CO, consisting of various functional departments deals with mainly policy formulation, setting of targets and monitoring of performance. The Bank has set up 13 Zonal Offices to exercise immediate supervision and control over the 59 Regional Offices, which in turn supervise the branches under their jurisdiction. The Bank has a network of 4720 plus branches, spread across the length and breadth of the country with presence in all the States and Union Territories. The Bank has also established its Wide Area Network at 4500 plus locations all over India covering administrative and branch offices and is planning to enlarge it

during the current year.

The Bank also has specialized branches catering to the specific needs of Retail customers, Industrial Units, Corporate Clients, Forex Dealers, Exporters and Importers, Small Scale Industries and Agricultural Sector. The Bank has sponsorship in 3 Regional Rural Banks (RRB).

Bank has implemented Core Banking Solution - B@ncs24 from Tata Consultancy Services Limited in 4720 branches. Bank is currently undergoing the process of setting up of Security operation Centre (SOC) to support and its existing Security Management.

1.3 PROJECT OBJECTIVE

Considering the fast-paced threats in the IT environment, Bank has decided to strengthen its Information Security set up as per the guidelines in the G. Gopalakrishna Committee Report & Recommendations on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, released in January, 2011 and RBI Circular on Cyber Security Framework in Banks dated 02 June 2016.

The scope of work is described in detail in Section 2 – “Detailed Project Scope” of this RFP document. Bank seeks comprehensive proposals from "Bidders" who have the capabilities to meet The Bank's requirements and have a serious interest in providing the required services. This RFP provides information on Bank and the scope of work, and instructions for the preparation and submission of the RFP Response by the Bidder to perform the scope of work.

Bank envisions selecting the Bidder who will procure, implement and provide comprehensive onsite warranty support for the required security solutions along with any Hardware components if required.

The objectives of this Request for Proposal (RFP) are:

- **Scope Definition:** To present the eligible Bidders with understanding of Bank's requirements aiming for Network & Security Solutions.
- **Background Information:** Provide the background information on existing business applications, underpinning IT infrastructure and services provided to support the business functions and operations.
- **Proposal Request:** To invite detailed proposals from Bidders as per the objectives defined in this RFP and adhering to stipulated terms and conditions.
- **Bidder Selection:** To shortlist Bidders for comprehensive technical and commercial evaluations and award the contract to the selected Bidder, taking into consideration evaluation parameters defined in this RFP.

The Successful Bidder shall be the single point of contact for all products and services offered, as described in the scope of work, and will be fully responsible for the overall delivery, project management and co-ordination with different stakeholders as specified in sections below.

The term of the Contract shall be for the period of 5 years from the day of acceptance of the Purchase Order.

1.4 PROJECT SCOPE

The Bidders who wish to take up the project shall be responsible for the following:

- Procurement of the necessary solutions and the corresponding hardware, software, database etc. required for implementing these solutions as mentioned in Appendix 1 Form B 01 – Bill of materials to the stipulated locations of the Bank
- For all the Security solutions mentioned in the in Appendix 1 Form B 01 – Bill of Materials, Bank has provided the scope for these solutions section 2.1 & minimum technical specification in Annexure 7 (Minimum Technical Specifications). The solutions proposed by the Bidder should comply with these minimum technical requirements
- Implementation of the respective solutions at Bank including configuration, customization of the products as per the Bank's requirement
- Integration of the solutions with the SIEM to provide a comprehensive single dashboard view of the security risks/ incidents for Bank
- Work with the existing System Integrator(s) of the Bank to integrate the security solutions with existing application platforms, server and storage environment, enterprise network, security solutions, ticketing tools etc.
- Development of operating procedures in adherence with Bank's policies
- Adherence to agreed Service Level Agreements (SLA) and periodic monitoring and reporting of the same to Bank
- Continual improvement of the Security Operations as defined in the SLA
- The Bidder is required to maintain the supplied components for the period of contract
- The Bidder shall be solely responsible for the sizing of these solutions to cater to the Bank requirements for the period of contract

1.5 PROJECT TIMELINES

The successful Bidder is expected to adhere to the following timelines concerning the implementation of the solutions/services in Bank:

Sl. No.	Time Activity	T	T+1	T+2	T+3	T+4	T+5	T+6	T+7	T+8	T+9
	Purchase Order										
1	Advanced Threat Prevention										
2	Host Intrusion Prevention System										
3	Application Change Control										

Sl. No.	Time	T	T+1	T+2	T+3	T+4	T+5	T+6	T+7	T+8	T+9
4	Mobile Device Management										
5	DDOS Mitigation solution										
6	Network Access Control										
7	Digital Rights Management										
8	Endpoint Encryption										
9	IT security GRC										
10	Brand Protection										
11	Decoy										
12	API Management										
13	Application Security Testing										
14	Vulnerability Management										
15	Firewall Analyzer										
16	Data Loss Prevention										

“T” denotes the date of release of PO to the Bidder. For example, T+3 represent that the solution

needs to be implemented within 3 months of the release of the P.O.

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 a need arises.

1.6 SCHEDULE OF EVENTS

Sl. No.	Event Name	Remarks
1	Name of RFP	Supply, Installation & Maintenance of Security Solutions
2	Date of Issue of RFP	31 October 2017
3	Download RFP documents	RFP to be purchased from DIT, Central Bank of India
4	Price of RFP – non refundable	INR 5,000/- (Rupees Five Thousand only)
5	Bid Security (EMD)	INR 2,00,00,000/- (Rupees Two Crore only)
6	Performance Bank Guarantee To be submitted as per format of Appendix 2 Form A 06 with the Technical Bid	10% of the 5 years TCO of the Project
7	Date of pre-bid meeting	10 November 2017 at 1500 hours
8	Last date to receive all the queries	08 November 2017
9	Email address & Contact details	Name: Suryanarayanan.K Designation: CISO Email ID: 1) infosec@centralbank.co.in 2) sminfosec@centralbank.co.in 3) smitpurchase@centralbank.co.in Office Number: 022-67123583, 022-67123571
10	Last date & time for submission of bids	30 November 2017 at 1500 hours
11	Date & Time of opening of Technical bid	30 November 2017 at 1530 hours
12	Address of submission of bids	In the Drop Box Kept at the 1st Floor Or Chief Manager – DIT, 1st floor, Central Bank of India, Central Office, Department of Information Technology, Plot no. 26, Sector 11,CBD Belapur, Navi Mumbai – 400614
13	Venue for presentation, pre-bid meeting & opening of bids	1st Floor DIT, Plot no. 26, Sector 11, CBD Belapur, Navi Mumbai – 400614
14	Date, Time & Venue for Reverse Auction Process	To be Notified later to the eligible Bidders

1.7 PRE BID MEETING

- Bidders, who have purchased the RFP, are only allowed to attend the pre-bid meeting. If any Bidder chose not to attend the pre-bid meeting, their queries if any may not be entertained by the Bank, However, they can participate in the RFP process.
- All queries / requests for clarification from Bidders must reach us by e-mail or in person before 08 November 2017.
- If the Bidder have any queries or require any clarification, Bidder should request the clarification from the Bank in the format provided in “Appendix 2 Form A 02 - Comments on T&C” for Terms & conditions related queries /clarifications and in “Appendix 2 Form A 03 - Query Format” for technical or other non – Terms & condition related queries / clarification. No clarification or queries will be entertained in any other format.
- The Bank reserves the exclusive right to make any amendments / changes to or cancel any of the above actions or any other action related to this RFP.
- The Bidder is required to provide a detailed strategy to the Bank; the activities mentioned above are indicative but the timelines for procurement and delivery should be maintained. Hence, if the Bidder has a quicker and effective solution the same may be discussed and agreed by the Bank.
- Any modification of the RFP, which may become necessary as a result of the Pre-Bid meeting, shall be made by the Bank exclusively through the issue of an Addendum and will be published on Bank’s website for information to all prospective Bidders.
- Non-Attendance at the Pre-Bid Meeting will not be the cause for disqualification of a Bidder.

2. DETAILED SCOPE OF WORK

2.1 GENERAL

Bank has decided to purchase the security solutions that will be integrated in the SIEM solution for monitoring as part of the on premise Cyber Security Operations Center (C-SoC) to enhance the existing security landscape of the Bank. The Scope includes procurement, implementation and integration of the solutions into the SIEM. The objectives of the security solutions is as below.

The principles that form the underlying platform for the SOC Services are as follows. The services offered should follow from these principles. The Bidder is expected to adhere to these principles while submitting their response:

2.1.1 FUNCTIONAL PRINCIPLES

The intent for Services/ Solutions is covered in the below functional principles:

- **Prevention & Identification of Information Security Vulnerabilities:** The services/ solutions should be able to identify information security vulnerabilities in Bank's environment and prevent these vulnerabilities
- **Incident Management:** Reporting of information security incidents using appropriate tools. Track and monitor the closure of these information security incidents and escalation of these incidents to appropriate teams/ individuals in the Bank
- **Continuous Improvement:** Continuously improve services/ solutions as per the requirements from the Bank.

2.1.2 SCALABILITY PRINCIPLES

All the services/solutions offered should be modular, scalable, and should be able to meet Bank's requirements during the period of contract.

2.1.3 AVAILABILITY PRINCIPLES

All the services/solutions in scope needs to be designed and implemented with adequate redundancy and fault tolerance to ensure compliance with SLAs for uptime as outlined in this RFP.

2.1.4 PERFORMANCE PRINCIPLES

It should be ensured that neither during installation nor during operations of the security solutions any of the existing infrastructure/ business of the Bank is impacted.

Based on the above principles, Bank has envisaged the following security solutions, required over and above their current existing set of solutions to enhance the robust monitoring by integrating with the SIEM that are compliant with ISO 27001, PCI-DSS, OWASP etc.

- Advanced Threat Prevention (ATP)

- Host Intrusion Prevention System (HIPS)
- Application Change Control (ACC)
- Mobile Device Management (MDM)
- Distributed Denial of Service (DDOS)
- Network Access Control (NAC)
- Digital Rights Management (DRM)
- Endpoint Encryption
- IT Security Governance, Risk and Compliance (ITGRC)
- Brand Protection
- Decoy (Honey Pot)
- API Management
- Application Security Testing
- Vulnerability Management
- Firewall Analyzer (FA)
- Data Loss Prevention (DLP)

2.2 SCOPE OF WORK FOR EACH SECURITY SOLUTIONS

This section covers the broad set of requirements for all the solutions to be deployed at Bank.

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.

All the proposed security equipment/devices should be IPv6 compliant from Day 1.

The Bidder is required to provide the following as part of the solution to the Bank:

- Bidder has to ensure that the end to end installation, configuration, parameterization, customization, implementation and integration has to be mandatorily carried out by the OEM for all the solutions that needs to be implemented at central site i.e. DC & DR. For branch level activities, bidder can perform the installation, configuration, parameterization, customization, implementation and integration of the solution deployed at branches/other offices.
- Solutions as defined in the section: "Solutions Required"
- Work force to manage the operations for the solutions in scope and to ensure SLA compliance
- Bank reserves the right not to procure/implement any or all of the proposed tools mentioned in this RFP. In such cases, cost for tools procured by the Bank would only be payable to the Bidder.

2.2.1 ADVANCE THREAT PREVENTION

The proposed advanced threat prevention solution should be able to address the following key areas but not limited:

- Detect and prevent advance targeted malware in the network infrastructure (covering channels like Web, Email) and perform analysis on premise and no information shall be sent outside the Bank
- Should support unlimited endpoints on a single ATP Appliance or multiple or under HA mode or stand-by mode.
- The ATP solution should have the following technology for detecting unknown security threats:
 - ✓ Prevention from Zero Day attack
 - ✓ Inspection of SMTP, POP3, IMAP traffic
 - ✓ Ransom ware Detection & Prevention
 - ✓ Sandboxing capabilities of necessary Operating Systems as deployed in the network
 - ✓ Automated Malware Analysis
 - ✓ Real-Time Threat detection
 - ✓ Solution should be deployed on premise and along with on premise sandboxing capability
 - ✓ Solution should be able to detect the persistent threats which come through executable files, PDF files, Flash files, RTF files, any type of file
- Solution should support all the industry standard protocols for inspection.
- Solution should have centralized architecture with web or GUI based dashboard console to monitor, reporting, notification, maintaining and policy push for the registered users centrally.
- The solution should be able to address all aspects of the Advanced Threat protection(ATP) lifecycle, including: Blocking known malware sources, blocking known malware, identifying and blocking unknown or zero-day malware within an hour, protecting against client-side vulnerabilities, blocking command and control back-door traffic, blocking server-side vulnerabilities, and advanced application and user control.
- Solution shall support the following remote access capabilities on its management interface via HTTPS or SSH access
- Solution shall provide the malicious files management UI such as suspicious file downloads for further investigation or sample submission to different Security OEM's.
- Solution shall support role-based administration such as Administrator, Malware Analyst, Database Reader, and Read-only access users.
- Solution shall provide forensic evidence on the infections activity within the network as follow: Event timestamp, network events in sequence, packet capture of suspicious communication, malware behaviors, malware type, severity, source and destination of attack.
- The proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single appliance.
- Solution should have built in capabilities to add exceptions for detections
- Solution should have capabilities to configure files, IP, URLs and Domains to Black list or white list
- Shall detect and monitor the traits or actions of suspicious files by identifying the following: Registry accessed File accesses, File modifications and Network communication.

- Solution should have built in various reports and can create custom reports like Executive report, Infection life cycle report, Top 10 reports for various category and Health reports etc.
- Solution should provide reports with (but not limited to) HTML/CSV/PDF formats
- Solution should be able to schedule reports and also provide the flexibility to generate on-demand reports in daily/weekly/monthly/yearly or specific range (by day and time)
- Solution should have a minimum usable storage of 500GB

SOLUTION IMPLEMENTATION

- Implement the solution across the Bank
- Configuration and deployment of policies as per the Bank's requirement

TRAINING

- 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 ATP policy configuration, alert monitoring, and etc. post implementation.

SOLUTION INTEGRATION

- Integrate ATP with SIEM to generate alerts for any ATP violations.
- 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.

2.2.2 HOST INTRUSION PREVENTION DETECTION (HIPS)

The proposed Host intrusion prevention Detection solution should be able to address the following key areas but not limited:

- The solution should be able to protect servers/applications from unknown malicious attacks and against unknown zero-day attacks with anomaly detection provision
- The proposed solution should be compatible with the multiple operating systems viz. Solaris, Linux, AIX, UNIX, Windows.
- The solution should protect against vulnerabilities introduced from mobile users.
- The solution must address and mitigate the all OWASP application security vulnerabilities
- The solution should be compatible with virtualized and physical server platforms
- The solution should be able to automatically block attackers IP address
- The solution should get automatic security updates
- The solution should perform log analysis, integrity checking, rootkit detection, time-based alerting and active response. It should help to detect attacks, software misuse, policy violations and other forms of inappropriate activities.
- The solution should be able to monitor multiple systems, with one system being the HIPS server and the others the HIPS agents that report back to the server.
- The solution needs to have the following minimum features:

- ✓ Time to Time Signature updates
- ✓ Monitoring and prevention from Intrusion attack
- ✓ Monitors specific system
- ✓ Detects attacks that network-based systems miss
- ✓ Well-suited for encrypted and switched environments
- ✓ Near-real-time detection and response

SOLUTION IMPLEMENTATION:

- Implement the solution across the Bank.
- Configuration and deployment of policies as per the Bank's requirement.

TRAINING:

- 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 HIPS policy configuration, alert monitoring, and etc. post implementation.

SOLUTION INTEGRATION:

- Integrate HIPS with SIEM to generate alerts for any HIPS violations.
- 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.

2.2.3 APPLICATION CHANGE CONTROL

The proposed Application change control solution should address the following key areas but not limited:

- The proposed solution should be compatible with the multiple operating systems viz. Solaris, Linux, AIX, UNIX, Windows.
- The proposed solution should have File Integrity Monitor for files and directories on critical servers
- The solution should have necessary change management policies to be deployed in conjunction with the Bank's internal processes
- The proposed solution should protect the Bank's applications and monitor all changes to ensure security and availability of all critical Banking infrastructure vide following solutions:
 - ✓ Application change control Security for critical servers
 - ✓ File Integrity Monitor for files and directories on critical server
- The proposed solution should have ability to protect against zero-day and advanced persistent threats without signature updates, it should be able to identify and whitelist all in-scope applications dynamically

- The proposed solution should have ability to prevent running application from advanced persistent threats
- The proposed solution should have ability to prevent any malicious or unauthorized codes from execution on the servers without affecting the server performance.
- The proposed solution should have ability to allow new software added through your authorized processes only
- The proposed solution should have support for virtualized environments
- The proposed solution should have ability to ensure protection on unpatched servers even if critical vulnerabilities exist on them
- The proposed solution should have capability to continuously capture changes on server name, file name, time of change, change type, content and provide forensic data for Auditing and regulatory purposes
- The proposed solution should have ability to detect and prevent all unauthorized changes to critical system files, directories, and configurations as per RBI guidelines
- The proposed solution should be able to integrate with third party change management solutions for approval purposes
- The proposed solution should have ability to monitor integrity of files and folders for PCI and other compliance requirements like RBI Guidelines

SOLUTION IMPLEMENTATION

The Bidder is expected to perform following activities:

- The Bidder needs to demonstrate the technical capabilities and features of the solution and also need to show case the working of the solution in Bank's environment before implementing
- Design & size the solution at DC and DRC for Internet Banking, AML, Eximbill and ASBA
- Configuration and deployment of policies as per the Bank's requirement

TRAINING

- 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 ACC policy configuration, alert monitoring, and etc. post implementation.

SOLUTION INTEGRATION

- Integrate ACC solution needs to be integrated with the following solutions:
 - ✓ Internet Banking
 - ✓ AML
 - ✓ Eximbill
 - ✓ ASBA
 - ✓ Mobile Banking

2.2.4 MOBILE DEVICE MANAGEMENT

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:

- Configuration of the solution balancing critical document access requirements with data security assurance
- Tying mobility to strategic business objectives
- Identifies key business processes that can be improved with mobilization
- Defines business process improvements
- Devise business and technical alignment with Bank's requirement
- To implement every aspect of the identified and designed mobility initiative, including architecture and systems integration
- Assists with device management and configuration
- Provides different devices application hosting options
- Provides help desk services
- Scalable, so new users and increasingly sophisticated devices can be accommodated easily

Below is number of devices to be covered by the MDM solution, the solution is to be deployed in standalone mode at both DC and DR.

Sl. No.	Description	Number of Users
1	Current No. of mobile users	1000
2	Additional Scalability over the period of 5 years	2000

The Bidder is expected to perform the following activities:

SOLUTION IMPLEMENTATION

- Implement the solution for the identified devices.
- Configuration of the required policies

TRAINING

- 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.

SOLUTION INTEGRATION

- Integrate MDM with SIEM to generate alerts for any MDM violations.
- The 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
- The Bidder needs to ensure the proposed solution is configured to generate events for monitoring through SIEM

2.2.5 DISTRIBUTED DENIAL OF SERVICE (DDoS)

The proposed DDoS solution should address the following key areas but not limited:

- Prevent all types of DDoS attacks (volumetric, protocol & application) such as, but not limited to, UDP Flood, ICPM Flood, SYN Flood, Smurf DDOS, Slowloris, HTTP Flood, Zero-day attacks, TCP exhaustion, etc. that impact the services hosted on Internet.
- The solution should be able to mitigate the effects of DDoS attacks over Internet links commissioned in our Data Centre.
- The Solution should identify the root cause of the attack & take preventive action to avoid facing similar type of attacks again.
- The solution should handle up to 2 Gbps of throughput in High Availability in DC and DR
- Solution should detect the attack irrespective of the type of attacks such as volumetric, layer 2, 3, 4 or 7 using the solution provided by them
- Proposed solution should have capability of Detection and Mitigation of DDoS attacks.
- constantly monitor the behavior of the application visitors

The Bidder is expected to perform the following activities:

SOLUTION IMPLEMENTATION

- Implement the solution as per Bank's requirement
- Configure policies as per Bank's requirement.

TRAINING

- 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 DDoS policy configuration, alert monitoring etc. - post implementation.

SOLUTION INTEGRATION

- Integrate DDoS solution with SIEM to generate alerts for any violations
- The Bidder shall be responsible for providing the operational and maintenance training to the identified IT staff of the Bank as and when required by the Bank. The Bank shall provide adequate support to the Bidder for the purpose of integration.

2.2.6 NETWORK ACCESS CONTROL

The proposed Network Access Control solution should be able to address the following key

areas but not restricted:

- The Bank intends to procure a Network Access Control solution which is an automated security control platform that can monitor and control everything on the network—all devices, all operating systems, all applications, all users.
- The solution shall let employees and guests remain productive on the network while critical network resources and sensitive data remain protected. Based on third-generation network access control (NAC) technologies, the solution shall be easy to install, manage, configure and upgrade.
- NAC shall provide following:
 - ✓ Visibility into user identities and device types
 - ✓ Guest user self-enrollment
 - ✓ Easy access to WPA2 secure wireless and wired networks
 - ✓ Real-time policy assessment
 - ✓ Dynamic role-based enforcement
 - ✓ Guided Self-Remediation Process
- NAC solution deployed shall allow only authorized and compliant devices to access and operate on Bank's network. The Bidder shall design the NAC solution such that the Bank does not need re-architecture of the network or upgrade/ replacement of the network devices
- In case of failure of NAC appliance/ software, the Bidder shall provide redundant solution in no more time than 4 hours for any location where ever NAC is deployed.
- The Bidder is required to supply, implement & maintain NAC for:

Sr. No.	Locations	No. of Locations	Additional Scalability for Next 5 years
1	Endpoints (Includes DC, DRC, Branches. ATMs and Kiosks)	40000	1000

- The solution should be scalable to support additional 1000 End Points during the of the contract
- The solution is to be deployed at DC in HA mode and at DRC in HA mode.

SOLUTION IMPLEMENTATION

- Implement the solution for the identified devices
- Configuration of the required policies

TRAINING

- 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 NAC policy configuration, alert monitoring, and etc. post implementation.

SOLUTION INTEGRATION

- Integrate NAC with SIEM to generate alerts for any NAC violations.
- The 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.
- The Bidder needs to ensure the proposed solution is configured to generate events for monitoring through SIEM

2.2.7 DIGITAL RIGHTS MANAGEMENT

The proposed Digital Rights Management solution should be able to address the following key areas but not limited:

- The proposed solution should work for sharing files with internal & external users.
- The proposed solution should work for sharing files with offline & online mode.
- The proposed solution should integrate with internal and external or third party application.
- The proposed solution should have Web Client functionality.
- The proposed solution should have feature of Uploading file in web client.
- The proposed solution should have the option for allowing the console user to set start and end date/time for each policy deployed
- The proposed solution should apply control policy to the share folder of server (hot folder policy) / application server, which will be access by third party / Bidder.
- The proposed solution should be able to integrate using API with at least 3 applications initially and with the capability to perform end to end encryption/decryption of the applications
- Solution should have Protection of file with desired permission:
 - ✓ Read-only
 - ✓ Restricted
 - ✓ Unlimited
 - ✓ Printing protection
 - ✓ File expiry by Number of days/Minutes/Hours
 - ✓ File expiry by date
 - ✓ Screen Sharing
 - ✓ Copy past should not work from the restricted documents
- The proposed solution should have capability to classify the data created in MS-word, MS-Excel, pdf, txt, rtf, MS-pptx. etc.
- The proposed solution should provide classification of documents based on their sensitive levels as Public, Internal, Private, and Confidential
- All the policies defined for various classification should get implemented to the data based on the classification level selected
- The proposed solution should be able integrate with Active Directory, Existing Data Leakage Prevention systems and SIEM solutions
- Allow console user to define different policies

SOLUTION IMPLEMENTATION

- Implement the solution across the Bank.
- Configuration and deployment of necessary policies as required by Bank.

TRAINING

- 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 DRM policy configuration, alert monitoring, and etc. post implementation.

SOLUTION INTEGRATION

- Bidder shall integrate the proposed DRM solution across the Bank
- Integrate DRM with SIEM to generate alerts for any violations.

2.2.8 ENDPOINT ENCRYPTION

The proposed solution should address following features but not limited to:

- Full Disk Encryption (Drive Encryption)
- File and Folder Encryption (FFE)
- Removable Media Encryption (RME)
- Solution should have centralized management through standard server-based or web console for management and should be able to enforce policies
- The solution should allow for installation in a virtualized environment.
- The solution should be able to encrypt files/folders on Desktops, mobile Laptops, network drives, Smartphone's and external removable media (USB pen drives, CD/DVDs) with sector based encryption
- The solution should be Encrypting with the read/write processes on the host computer
- Proposed solution (of OEM) should have their own encryption engine for the supported OS mentioned
- The proposed solution should support on the fly management of policies and should be replicated almost immediately to the encrypted workstations
- The solution should allow for Segregation of roles with different access levels for administrators
- The proposed solution should be able to do automatic encryption with no requirement for user intervention when all files copied onto those devices.
- The proposed solution should be able to identify and verify authorized users by using strong multifactor authentication
- The proposed solution should ensure that specific files and folders are always encrypted, regardless of where data is edited, copied, or saved (Persistent File and Folder Encryption)
- The proposed solution should do automatic encryption and protect files by dragging them into encrypted folders
- The proposed solution should be able to do removable media encryption that doesn't take up entire volume. (container / partition)
- The proposed solution should be able to create Password protected encrypted container with a Media Viewer for sharing information with authorized users that don't have Encryption client installed
- The proposed solution should be able to reset password created for removable media encryption
- The solution should have capabilities to have Self-Extracting Files - Send encrypted email attachments and allow access to the attachment without requiring the recipient to install any additional software

- The proposed solution should support AES 256-bit encryption that is used for the full disk encryption on a computer from day 1
- The solution should be Compliance - Protect your data with an endpoint encryption solution that is FIPS 140-2, Common Criteria EAL4, BITS, AES validation
- The solution should be able to provide compliance report
- The solution should be able to decrypt the contents and update the share folders only to the users with a matching encrypting key in network based encryption – Where the data is encrypted on a share on a File Server
- The solution should have ability to dynamically provision keys and key files
- The solution should have recovery Tool to allow for unlocking encrypted drive to recover data without decryption in case of OS corruption and ability to attach encrypted disks to another workstation and unlock drive
- Solution should do not prevent repair of bad sectors on non-SED drives (Self encrypted drives)
- Encrypted Removable Media should be accessible to third party users without installation of any application or plugin
- The encrypted External Media should be accessible both on Windows, Linux and Mac operating systems
- The proposed solution should allow for partial encryption of Removable Media without touching or affecting existing data on the drive. (The data remains on unencrypted portion of the media)
- Encrypted Removable must be transparently accessible by the employees without any password prompt
- The solution should be able to provision Disk Access Control for Removable Media – Options for:
 - ✓ Read Only
 - ✓ No Access
 - ✓ Read Only unless Encrypted (To prevent data leakage)
- The solution should have ability to customize user message prompt to provide approved message or instructions prior to performing removable media encryption.
- The solution should provide centrally log and capture all filenames written to external encrypted USB media
- Encryption should be Sector based encryption i.e. every byte of data is encrypted including temp, paging, deleted files, and the Windows registry
- The solution should support SED (Self Encrypting Drives) with support for OPAL standard
- The solution should have encryption conversion process tolerates interruptions i.e. power Outages, without data loss
- The solution should support for Cryptoterase to remotely wipe the device encryption key (across the WAN)
- The solution should provide automatic enrollment of owner of workstation without IT Support or Helpdesk involvement

SOLUTION IMPLEMENTATION

- Implement the solution on all the endpoint systems including DC, DRC, Branches, CO etc. as per Bank's requirement
- Configure policies as per Bank's requirement

TRAINING

- 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 all three encryption configurations, alert monitoring etc. - post implementation

SOLUTION INTEGRATION

- Integrate Endpoint Encryption solution with SIEM to generate alerts for any violations
- The Bidder shall be responsible for providing the operational and maintenance training to the identified IT staff of the Bank as and when required by the Bank.

2.2.9 IT SECURITY GOVERNANCE RISK AND COMPLIANCE

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

- 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
- Effective, ongoing controls and compliance management. Focus resources on high-impact processes, regulations, and risks to get continuous insight
- 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.
- 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).
- 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.
- 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.
- 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

- Scalable (capable of implementing one module/service at a time and adding users as needed).

SOLUTION IMPLEMENTATION

- Implement the solution across the Bank
- Design and Configuration of risk and compliance policies as per Bank's requirement
- Provide complete consultancy for implementing the solution across the Bank

TRAINING

- 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 IT security GRC policy configuration, alert monitoring, and etc. post implementation

SOLUTION INTEGRATION

- Bidder shall 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

2.2.10 BRAND PROTECTION

The proposed Brand Protection solution should be able to address the following key areas but not restricted:

- 24x7 anti-phishing, anti-Trojan, and anti-malware service to scan critical websites and Mobile Apps identified by Bank for the tenure of the project.
- Any newly launched websites and Mobile Application by the Bank in future to be scanned without any cost incurred to the Bank
- The solution provider should be able to Initiate the responses as per Bank's request
- The Bidder needs to ensure that the solution should be able to takedown websites and Mobile App as per Bank's request
- Access to Dashboard view of the "risks and threats" identified through the Anti-Phishing and threat intelligence services
- Monitoring of all major mobile application marketplaces for counterfeit, copycat apps, or apps infringing trademarks, linking to pirated content, attempting phishing attacks or distributing malware
- Prompt submission of enforcement notices and for the removal of rogue or infringing applications
- Bidder must have capability for monitoring of similar sounding domain name registrations and alerting the Bank if this is detected

The Bidder is expected to perform the following activities:

SOLUTION IMPLEMENTATION

- Deploy the Brand Protection services for DC and DR location
- Configure the Brand Protection policies
- Quarterly reports must be submitted for Banks's review which highlights the threats, risks and respective mitigation actions taken.

TRAINING

- 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 Brand Protection policy configuration, alert monitoring, problem mitigation and etc. post implementation.

MONITOR

- Bidder should ensure the maintenance of the solution and provision of logs on weekly basis for review with the Bank.

2.2.11 DECOY (HONEY POT)

The proposed Honey Pot solution should be able to address the following key areas but not limited:

- Effectively create a replica copy of the Bank's existing internet-facing landscape
- Hacking incentive of the proposed decoy ecosystem should be as equivalent to present exposed incentive of the Bank
- The intended solution must safeguard the Bank against a target DDoS attack, and also act as a layer of defense for attacks based on new-vulnerabilities, Anti phishing attacks, data theft and zero day attacks
- Should provide real time Alerts
- The solution should be able to integrate with the Active Directory

The Bidder is expected to perform the following activities:

SOLUTION IMPLEMENTATION

- Implement the solution across the Bank's internet facing landscape and any other critical service as deemed by the Bank.

TRAINING

- 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 Honeypot policy configuration, alert monitoring, and etc. post implementation.

SOLUTION INTEGRATION

- Integrate the honeypot solution with SIEM to generate alerts for any violations.
- 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.

MONITORING

- Bidder should ensure the maintenance of the solution and provision of logs in integration with the SIEM for review with the Bank.
- 24*7 monitoring of all the websites and services under the architecture of Honeypot with no exceptions

2.2.12 API MANAGEMENT

The envisaged API Management solution should provide policy and governance framework with following API infrastructure platform features, however, not restricted to:

- The Application should be sized for Active- Active cluster at DC & Active-Active cluster at DR so that the solution and infrastructure can fall back on each other. DC – DR replication should be available as part of the solution so that in case of switch over the complete solution should seamlessly work.
- Proposed solution should be highly scalable architecture, initially supporting 1000 transactions per second (TPS) considering average payload of 30 Kb and 500 concurrent users. Bidder should also create test and development setup for 6 users simulating near production functionalities
- Key point of entries, through the APIs, need to be protected against vulnerabilities or security flaws in the system
- Central repository governing the security policies of the published APIs. The security policies would govern the requirements of the transport level security, SLA parameters, throttling parameters and authorization metadata
- Dashboard providing an insight to all the published endpoints and related SLA parameters
- Versioning of the APIs with ability to host multiple versions and block/retire specific versions
- Key server to manage access tokens and provisioning of the API to the consumers
- Workflow to publish APIs in UAT/Sandbox/Production environments with ability to implement user approval based publishing
- Configurable business event and audit logging that can be adjusted as per the requirements
- The proposed solution should support TCP/IP adaptors and OSGI adaptor.
- Analytics and reporting capabilities for active monitoring of the API usage

SOLUTION IMPLEMENTATION

- The Bidder needs to demonstrate the technical capabilities and features of the solution and also need to show case the working of the solution in Bank's environment
- Implement the solution as per Bank's requirement
- Configure policies as per Bank's requirement.

TRAINING

- 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 API Management solutions operations – post implementation.

- The Bidder shall be responsible for providing the operational and maintenance training to the identified IT staff of the Bank as and when required by the Bank.

SOLUTION INTEGRATION

- Integrate API Management solution with SIEM to generate alerts for any violations
- The primary responsibility of integration of new solutions with existing SIEM lies with the Bidder/SI selected through this RFP. Adequate support shall be provided by the existing SIEM System Integrator for the purpose of integration.

2.2.13 APPLICATION SECURITY TESTING

The proposed Application security testing solution should also provide capability of Static Application Security testing and Dynamic Application Security testing to identify potential security issues with its applications prior to going live on production and post-go-live on production. The proposed solution should address the following key areas but not limited:

- Comprehensive approach specifically designed to proactively mitigate or prevent the exploitation of vulnerabilities which exist in the systems.
- Outline and configure application security policies
- Discover existing vulnerabilities in applications
- Analyze current level of security & rank vulnerabilities by threat level/remediation actions required
- Mitigate the causes of vulnerabilities
- Active analysis of the application for any weaknesses, technical flaws or vulnerabilities
- Perform source code analysis and application security testing to identify coding and design flaws
- Perform application security testing of the application to identify security vulnerabilities
- Demonstrate that the application meets the specified security requirements
- Ability to unify the organization of vulnerabilities and maps them to standards such as OWASP, SANS, CWE, and FISMA, etc.

Generate reports on vulnerabilities identified and recommendations on how to fix the found issues until final closure

SOLUTION IMPLEMENTATION

The Bidder is expected to perform following activities:

- Deploy the Application Security testing to test the critical Applications
- Configure the Application Security testing policies as per Bank's requirement.

TRAINING

- 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 Application Security Testing policy configuration, alert monitoring, and etc. post implementation.

SOLUTION INTEGRATION

- Integrate Application Security testing with SIEM to generate alerts for any Application Security violations and provide a correlated view of threats and vulnerabilities associated with them along with remediation mechanism.
- The responsibility of integration of the application security testing solution 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.
- Bidder is expected to perform application Security test on quarterly basis for the identified systems and provide reports for the same as per SLA. Also, if any new device is procured / or existing device ad-hoc application security testing to be performed as per Bank's requirement.

MONITORING

- Conduct Application security test quarterly and monitor & report events from Application security test tool and suggest/take appropriate action to the Bank on an on-going basis.
- Improve the policies configured on an on-going basis to reduce the occurrence of false positives.

2.2.14 VULNERABILITY MANAGEMENT

The proposed Vulnerability Management solution should also provide capability of Static Application Security testing and Dynamic Application Security testing to identify potential security issues with its applications prior to going live on production and post-go-live on production. The proposed solution should address the following key areas but not limited:

- Comprehensive approach specifically designed to proactively mitigate or prevent the exploitation of vulnerabilities which exist in the systems.
- Outline and configure vulnerability management policies
- Discover existing vulnerabilities
- Analyze current level of security & rank vulnerabilities by threat level/remediation actions required
- Mitigate the causes of vulnerabilities
- Maintain security through ongoing testing and discovery
- Vulnerability scanning has to be performed on a periodic basis for critical devices
- Active analysis of the application for any weaknesses, technical flaws or vulnerabilities
- Perform source code analysis and application security testing to identify coding and design flaws
- Perform application security testing of the application to identify security vulnerabilities
- Demonstrate that the application meets the specified security requirements
- Ability to unify the organization of vulnerabilities and maps them to standards such as OWASP, SANS, CWE, and FISMA, etc.
- Generate reports on vulnerabilities identified and recommendations on how to fix the found issues until final closure

SOLUTION IMPLEMENTATION

The Bidder is expected to perform following activities:

- Deploy the VM to monitor the critical devices
- Configure the VM policies as per Bank's requirement.

TRAINING

- 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 VM policy configuration, alert monitoring, and etc. post implementation.

SOLUTION INTEGRATION

- Integrate VM with SIEM to generate alerts for any VM violations and provide a correlated view of threats and vulnerabilities associated with them along with remediation mechanism.
- The responsibility of integration of the VM solution 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.
- Bidder is expected to perform VA on quarterly basis for the identified systems and provide reports for the same as per SLA. Also, if any new device is procured / or existing device ad-hoc VA to be performed as per Bank's requirement.

MONITORING

- Conduct VA quarterly and monitor & report events from Vulnerability manager and suggest/take appropriate action to the Bank on an on-going basis.
- Improve the policies configured on an on-going basis to reduce the occurrence of false positives.

2.2.15 FIREWALL ANALYZER

Bank has Firewalls in DC/DR infrastructure for securing data from unauthorized access and external threats. Currently the Bank utilizes various Next Generation Firewalls of different makes in its Network environment to protect, secure and prevent itself from external attacks. Frequent changes, up-gradation and improvements on these Firewalls are being undertaken to keep pace with the technological development.

As all the Firewall rule reviews are being done on a manual basis and this process needs to be automated. Bank intends to use the proposed Firewall Analyzer to optimize the Firewall Rules and maintenance of the same in order to achieve better utilization and productivity. The solution should also be able to automate the various Firewall rule based reviews using the Firewall Analyzer.

Policy Compliance

- The Bank Information Systems Security Policy (ISMS) requires that the Firewall rule base should be reviewed on a quarterly basis.
- The report of these rule base reviews also needs to be documented.

Audit Compliance

- These Firewall rule base review reports are required for the various audits including PCI-DSS, ISO 27001 etc.

Productivity Improvement

- Firewall rule optimization and maintenance is necessary in order to achieve better Firewall utilization and productivity
- Rule synchronization between DC & DR setup.
- Automated rule review will provide better reports.

The proposed Firewall analyzer should integrate with all the different makes of Firewalls available with the Bank with no exceptions. Following are the list of existing Firewalls which needs to be integrated with the analyzer:

Sl. No.	DC/DRC/NDS	Location	Cluster	Total Number of Units
1	DC	Mumbai	4	8
2	DRC	Hyderabad	3	6

Note:

The detailed information would be shared with the L1 Bidder.

SOLUTION IMPLEMENTATION

- The Bidder needs to demonstrate the technical capabilities and features of the solution and also need to show case the working of the solution in Bank's environment
- Implement the solution as per Bank's requirement
- Configure policies as per Bank's requirement.

TRAINING

- 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.

SOLUTION INTEGRATION

- Integrate proposed Firewall Analyzer with all different makes of the Firewall for optimization, maintenance and review of the Rules
- Integrate Firewall Analyzer solution with SIEM to generate alerts for any violations
- The Bidder shall be responsible for providing the operational and maintenance training to the identified IT staff of the Bank as and when required by the Bank.
- Post Implementation the Bidder as well as OEM shall integrate new device with Firewall Analyzer as per Bank's requirement
- Port shall be provided by the existing SIEM System Integrator for the purpose of integration.

2.2.16 DATA LOSS PREVENTION

- Bank intends to implement Data Loss Prevention solution at DC and DR and at branches and other Bank's office locations as a new initiative to prevent the loss of confidential Bank data/ Bank customer information that could leak out of the Bank and would enable Bank to reduce the corporate risk of the unintentional or intentional disclosure of confidential information.

- The Bidder is required to design & size the Data Loss Prevention (DLP) solution at DC and DR. The Bidder shall size the solution for the Bank's terminals that are connected to the Bank's network for accessing the proposed solutions at DC & DR.
- The Bidder is required to size, supply, implement & maintain network DLP at DC & DRC for the period of contract.
- The Bidder is required to supply, implement & maintain host DLP for 36515 endpoints for the period of contract. The solution should be scalable to support 40000 Endpoints during the tenure of the contract
- The Bidder is also required to install, configure & provide comprehensive onsite warranty & AMC/ATS services for the same over the tenure of the contract.
- The proposed Data Protection solution should be able to address the following key area:
 - ✓ Identify data leakage across all vectors, irrespective of policy being in place or not
 - ✓ Protect data
 - ✓ Have flexible control over Remediation of Data Leakage
 - ✓ Ease of Use and Quick to Deploy
- The Functional requirements of the Data Loss Prevention solution are:
 - ✓ Proposed Data Loss Prevention Solution should be able to provide controls that encompass the Network. The data loss solution should be able to start at the very basic level and progress to subsequent advanced levels of usage.
 - ✓ Data protection should also involve being able to identify known and unknown plug and play devices being connected to critical data resources. Also, the solution should seamlessly integrate with Encryption which should be intelligent enough to enforce Encryption of sensitive data.
 - ✓ The DLP solution should be able to go beyond known policies and provide Forensic capability on all historic data. Thus, the DLP should safeguard sensitive data and ensure compliance by protecting sensitive data wherever it lives—on the network or in storage systems, while saving time and money with centralized deployment, management, and reporting.
 - ✓ Quick Deployment capability and Single Management Console for configuring Uniform Policies across Network
 - ✓ Capability to monitor all traffic flowing out of the network, irrespective of Policies being in place or not
 - ✓ Ability to handle data being written on different types of media and option to monitor or prevent the same
 - ✓ Ability to seamlessly integrate with encryption and selectively encrypt data on the basis of designed policies
 - ✓ Enforce compliance over data sitting in different locations and be able to remediate
 - ✓ Employ different fingerprinting methods to signify sensitive data
 - ✓ Be protocol and port agnostic so as to tackle non-standard Data Transfer channels
 - ✓ Forensic capability of searching through all the past traffic
 - ✓ Capability to exert sufficient control on external devices being connected in the environment
 - ✓ Flexible reporting options for technical as well as high level reports
 - ✓ Multiple deployment options comprising of Hardware and Software
- Functional Requirement of Data Classification

- ✓ Identifying commonalities in critical information across multiple processes, and combined into higher level policy definitions.
- ✓ Confidential data types and risks based of classification
- ✓ Tagging of information asset with classification scheme
- ✓ Business impact valuation of information asset, artifacts
- ✓ Identification of risks and risk exposure
- ✓ Identify the category of data protection required for identified sensitive data
- The Bidder is required to monitor all relevant data leaving the Network and be able to create policy for protection of the same.
- The Bidder is required to locate all of the Sensitive data and classify it according to set process. The Bank or its appointed consultant will classify the data based on criticality.
- The Bidder is required to put in place prevention or protection rules for that data deemed necessary.
- The Bidder is required to install the data control for identifying any change in the critical files identified by the Bank.
- The Bidder shall configure integrity monitoring for the files and ensure write protection wherever necessary.
- There should be enough audit trail capability to identify drift in the document and all the relevant details like who made what changes and change details.
- Audit should allow for Reporting and Search capabilities.
- The OEM shall provide the training of the deployed solution to the Bank personnel for 1 batch with 10 personnel in each batch.
 - ✓ Provide training 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 team on DLP policy configuration, alert monitoring, etc. post implementation
- The DLP solution should duly meet the minimum technical requirements as specified Technical Requirements Annexure 7

SOLUTION IMPLEMENTATION

- The Bidder needs to demonstrate the technical capabilities and features of the solution and also need to show case the working of the solution in Bank's environment
- Implement the solution as per Bank's requirement
- Configure policies as per Bank's requirement.

TRAINING

- 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 DLP solutions operations – post implementation.
- The Bidder shall be responsible for providing the operational and maintenance training to the identified IT staff of the Bank as and when required by the Bank.

SOLUTION INTEGRATION

- Integrate DLP with SIEM solution to provide a single view of events generated.

- The primary responsibility of integration of new solutions with existing SIEM lies with the SI selected through this RFP. Adequate support shall be provided by the existing SIEM system integrator for the purpose of integration.

2.3 GENERAL RESPONSIBILITY OF THE BIDDERS AND OEM

- For the Security solutions mentioned in the Bill of Material in Appendix 1, Bank has provided the minimum technical specification in Annexure 7.
- 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 section 2.1 and Annexure 7 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.
- 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.
- 42U Rack with dual PDU and perforated doors (600x1000) and 1u swivel base foldable KVM Module with KVM switch having required ports and cables are also to be provided by the bidder.
- All the equipment should be Rack Mountable and should have dual Power supply units. LTO6 Tape Drive or 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.
- 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.

Bidder is required to carry out activities given in the following table:

Sr. No.	Phase	Nature of activity	Remarks	Primary Responsibility
1	Pre – Technical Bid submission	Proof of Concept of the following solutions prior to submitting the Technical Bid: • Application Change Control	The Bidder needs to provide Proof of concept of the solutions mentioned during the submission of the Technical Bid The Bidder needs to approach the Bank with their respective solution and provide a timeline and confirmation	Bidder
2	Planning	• Conduct Kick-off meeting • Identify project point(s) of contact • Identify Bank	Project Plan Project Governance	Bidder

Sr. No.	Phase	Nature of activity	Remarks	Primary Responsibility
		resources required to assist in deployment, policy walkthrough, testing, and installation. • Low Level Requirement Gathering • Project Planning		
3	Design	• OEM should execute design phase • OEM should develop and/or review and validate solution design/architecture documents which will include: • Solution overview and conceptual design • Detailed design and connectivity parameters • Create a User Acceptance Test Document	Design & Architecture Document Prerequisite Document User Acceptance Test Plan	OEM
4	Delivery	• Physical delivery of the security equipment/solutions as per Appendix 1 - Bill of Materials at DC, DRC, Branches and CO	The Bidder has to supply and deliver the security equipment/solutions mentioned in Appendix 1 - Bill of Materials at the respective Bank's site	Bidder/OEM
5	Installation & configuration	• Deploy solution • Complete initial configuration • Complete Integration with SIEM and other applicable applications • Documentation of installation and	The OEM is required to provide following deliverables as part of the this phase: Successful deployment solution Installation and Configuration Document Gap Assessment The Bidder/OEM is required	OEM

Sr. No.	Phase	Nature of activity	Remarks	Primary Responsibility
		configuration	to unpack, assemble, mount and boot the equipment and install the necessary service packs, patches, and fixes to the Operating System, set up and configure the equipment. Bidder to resolve any compatibility issues of sub-systems with OS, respective drivers, firmware, and any other cards to be installed if required. Bank will provide inputs/configuration details to the Bidder for configuring the equipment along with other required document and related architecture documents	
6	Optimize	- Fine-tuning of solution - Monitor and resolve issues - Provide an information knowledge-transfer workshop	Tuning policies. Policies override SOP Transfer of Information session	OEM
7	Deployment Confirmation and Validation	- This phase will comprise of deployment validation to be conducted by OEM. - In case OEM is not satisfied with the installation and configuration of product, they will submit their recommendation in form of a report to the Bank accordingly	Validation Report by OEM	OEM
8	Monitoring, Management & Sustenance	Post- deployment (after sign-off) Bidder will manage & monitor	Reports and Dashboards as per defined SLAs Go Live Operations	Bidder/OEM

Sr. No.	Phase	Nature of activity	Remarks	Primary Responsibility
		proposed solution • Facilitation & operation for all change management, upgrade, updates, etc. during contract period		
9	Warranty & AMC/ATS	• Provide warranty and AMC/ATS support for the tenure of the contract	The Bidder will be responsible for providing comprehensive onsite warranty support, back-to-back from the OEM to meet the Service Levels defined in Section 2.4	Bidder

The Bidder should take adequate care to avoid quoting security equipment that will become end of sale within 24 months of supply to the Bank and end of support within 7 years from the date of the submission of offer.

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 (Section 1.4 of this document). 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.

2.3.1 TRAINING

All trainings will be arranged by the selected Bidder/OEM in Bank's premise. Bank will provide training room along with required no. of PCs and projector. Rest all expenses will be borne by Bidder. In case there is need to conduct training at OEM/Bidder premises, Bank will provide only logistics.

- **Pre-Implementation:** Provide training to the identified Bank personnel/ SOC team on the product architecture, functionality and the design for each solution under the scope of this RFP.
- **Post Implementation:** Provide hands-on training to the Bank personnel/ SOC team on operations, alert monitoring, policy configuration, generation of reports, and analysis of the reports, Troubleshooting and familiarization of features and functionalities for all solutions independently.
- The Bidder shall provide comprehensive training manual, presentations, videos, lecture notes, hand-outs and other training documentation for all trainings. The training material should be in mandatorily in English.

- The Bidder may utilize the OEM resources in case the Bidder does not have adequately experienced resources for providing training.

2.3.2 IMPLEMENTATION & INTEGRATION

- Implementation of the specified solutions and necessary hardware requested by Bank and as per the technical requirement of the solutions. Selected Bidder to ensure that the proposed solution complies with all the technical requirements (Annexure 7) post implementation of each solution to which the Bidder responds as “Yes” in Annexure 7.
- 15 days before delivery of the solutions, the Bidder is required to review the Bank environment and specify any additional requirements that the Bank may need to provide for the implementation of the solution.
- The Bidder is responsible to ensure that the security solutions and their operations comply with Bank’s information security policies and industry leading standards (such as ISO 27001 ISO 22301, PCIDSS, etc.) and any applicable laws and regulations
- In addition, the Bidder is responsible for impact assessment and modification of solution operations at no extra cost, on account of any changes to applicable information security policies/ procedures / standards/ regulations.
- The support for all the solutions proposed should be provided for minimum 5 years. Whereas free upgrade should be provided for all solutions if the end of life occurs within the period of contract with Bank. The Updates/ Upgrades should be implemented within 6 months of release of the successor solution.
- Integrate each solution with the existing SIEM solution to provide a single view of events generated.
- In case end of life/end of support for any proposed solution including software, hardware, license and appliance is declared by OEM within contract period, Bidder shall provide upgraded version of the products without any additional cost to the Bank.
- Any interfaces required with existing applications/ infrastructure within the Bank should be developed by the Bidder for successful implementation of the solutions as per the defined scope of work.
- Bidder is responsible for developing and implementing the security configuration hardening of all the devices and software that are procured for Security Operations centre. Also, they have to periodically review the guidelines and configure as and when required.
- Bidder shall be responsible for timely compliance of all Device level audit (DLA) and Vulnerability Assessment (VA) audit observations as and when shared by the Bank.
- Post initial implementation, the Bidder is responsible for integrating any additional logs that the Bank may wish to monitor with the SIEM solution at no additional cost to the Bank
- The major and primary responsibility of integration of solution with SIEM lies with the Bidder selected through this RFP. The existing SIEM System Integrator and Bank shall provide adequate support for the purpose of integration with the SIEM.
- Development and implementation of processes for management and operation of the C-SOC including (but not limited to) the following processes:
 - ✓ Configuration and Change Management
 - ✓ Incident and Escalation management processes

- ✓ Daily standard operating procedures
 - ✓ Training procedures and material
 - ✓ Reporting metrics and continuous improvement procedures
 - ✓ Data retention and disposal procedures
 - ✓ BCP and DR plan and procedures for C-SOC
 - ✓ Security Patch management procedure
- Implement necessary security measures for ensuring the information security of the proposed C-SOC.
 - The technical bid should include an overview of the processes mentioned above.
 - ✓ Develop Escalation Matrix in order to handle Information Security Incidents efficiently.
 - ✓ Provide necessary documentation for the operation, integration, customization, and training of each of the solutions in scope.

2.3.3 CONTINUOUS IMPROVEMENT

- Improve the policies configured on an on-going basis to reduce the occurrence of false positives.
- Periodic health check should be carried out on-site, by the OEM every year to ensure the quality of implementation and operations. On need basis health checkup exercise shall be conducted.
- Bidder shall curtail the closure time for incidents and events, also ensure the periodic check-up reviews for the same.

2.3.4 SOLUTION ACCEPTANCE

The Bank/appointed consultant in coordination with the Bidder shall conduct an Acceptance test where in the Bidder has to demonstrate the implementation of the solution as per the technical requirements (Annexure 7) of this RFP. The Bidder shall submit the detailed reports of the test outcomes to the Bank.

2.3.5 SYSTEM INTEGRATION TESTING (SIT) AND USER ACCEPTANCE TESTING (UAT)

- There will be a User Acceptance Testing by the Bank for the tools deployed and C-SOC operations wherever applicable.
- The Bank shall commence the User Acceptance Testing as and when each and every products and services are made ready by the Bidder and a formal confirmation that the system is ready for UAT is submitted to the Bank. The results thereafter will be jointly analyzed by all concerned parties including OEMs.
- UAT will cover acceptance testing of all the product/services, integration with C-SOC tools (Primarily SIEM) and integration of C-SOC with all targeted devices/systems.
- Once UAT of all the tools of C-SOC are individually completed, then a System Integration Testing shall be carried out by the Bidder to ensure the complete interoperability of the C-SOC tools among themselves and integration with the existing infrastructure (targeted devices/systems) of the Bank as specified in the RFP.

- The Bidder is expected to make all necessary modifications to C-SOC solution including customizations, interfaces, appliances, integration, software etc., if there are performance issues and errors identified by the Bank. These deviations/ discrepancies/ errors observed will have to be resolved by the Bidder immediately.
- Complete acceptance has to adhere to the stipulated time lines.
- The solution will not be accepted as complete if any facility /service as required is not available or not up to the standards projected by the Bidder in their response and the requirement of this RFP.
- The Bank will accept the solution on satisfactory completion of the above inspection. The contract tenure for the Solution will commence after acceptance of the solution by the Bank.
- In case of discrepancy in facilities /services provided, the Bank reserves the right to cancel the entire contract.

2.3.6 WORKFLOW AUTOMATION

Selected Bidder must design a high level system integrated work flow pertaining to key security processes into the overall design of system which ensure minimum manual intervention

2.3.7 SLA COMPLIANCE

The Bidder shall ensure compliance with SLAs as defined in the RFP.

2.3.8 BUSINESS CONTINUITY

The Bidder is responsible for defining a DR/ BCP plan for the operations of each solution and ensure that periodic tests are conducted as per the testing calendar agreed with the Bank.

2.4 SERVICE LEVEL AGREEMENTS

This section describes the service levels that has been established for the Services offered by Bidder to the Bank. Bidder shall monitor and maintain the stated service levels to provide quality customer service to the Bank.

2.4.1 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 implementation fees 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 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, in case, the delay is more than 12 weeks. 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.

After acceptance of respective solutions by the Bank:

Sl. No	Service Area	Service Level	Penalty
1	All 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 individual monthly maintenance charges (AMC and ATS Charges). These penalties will be deducted against any payable amount by the Bank.
		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%
		Less than 70%	100%

SLAs for Solution Uptime

2.4.2 MONITORING AND OPERATIONS

Sl. No.	Service Area	Expected Service Level	Penalty
1	Incident Response	24x7 monitoring of all in-scope devices Categorization of events into Critical, High, Medium and Low priority shall be carried out in consultation with the selected Bidder during the contracting phase.	All Critical, High and Medium priority incident should be logged as incident tickets and responded as per below SLAs: Incident along with action plan/mitigation steps should be alerted to designated Bank personnel as per the below SLA: • 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 incidents identification. Update should be provided every 1 hour till the closure of the incident • Medium priority incidents within 60 minutes of the incidents

Sl. No.	Service Area	Expected Service Level	Penalty
			identification. Update should be provided every 4 hours till the closure of the incident. Penalty: SLA is measured on a monthly basis and the penalty is as follows: Critical Events: 95-99%: 10% of the Operations Cost for the Month 90-95%: 15% of the Operations Cost for the Month <90%: 20% of the Operations Cost for the Month High Priority Events: 95-99%: 5% of the Operations Cost for the Month 90-95%: 10% of the Operations Cost for the Month <90%: 15% of the Operations Cost for the Month Medium Priority Events: 95-99%: 1% of the Operations Cost for the Month 90-95%: 2% of the Operations Cost for the Month <90%: 5% of the Operations Cost for the Month 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.
2	Incident Resolution	Response and resolution of the identified incidents. Managing the devices and fine-tuning them so as to avoid and prevent further attacks.	The timelines required for resolution of Critical, High and Medium priority mentioned below: Disaster or Critical incidents within 60 minutes of the incident identification. Update should be provided every 15 minutes till the closure of the incident

Sl. No.	Service Area	Expected Service Level	Penalty
			- 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 every 4 hours till the closure of the incident. <u>Penalty:</u> - 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	Daily Reports: Critical reports should be submitted as and when required. Timings will be mutually decided. <u>Penalty</u> Delay in reporting for daily report for more than 1 hour shall incur a penalty of 3% of Operations Cost for the Month Weekly Reports: To be decided mutually <u>Penalty</u> Delay in reporting by more than 3 days for weekly reports shall incur

Sl. No.	Service Area	Expected Service Level	Penalty
			a penalty of 10% of Operations Cost for the Month Monthly Reports: 5th of each month <u>Penalty</u> Delay in reporting by more than 3 days for monthly reports shall incur a penalty of 10% of Operations Cost for the Month
4	Vulnerability Assessment and Penetration Testing (External & Internal)	- The Bidder is expected to provide Vulnerability Assessment Reports with remediation steps. - An incident needs to be logged for all vulnerabilities identified and the incident response SLA shall apply for these.	- To be conducted for identified devices once every month based on a calendar documented in coordination with the Bank to ensure that business operations are not impacted. - Ad-hoc scan to be conducted as and when required by the Bank <u>Penalty</u> - Delay in performing VA scan and providing report by more than 3 days shall incur a penalty of 10% of Operations Cost for the Month.
5	Continual Improvement	- 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.	- Quarterly reports need to be provided by the 5th day of each quarter beginning <u>Penalty:</u> - Delay in providing quarterly reports shall lead to 2% of the monthly C-SOC operation charges Reduction by 2% in the time for event response, quarter on quarter.
6	Periodic Review	The C-SOC project sponsor	Monthly meeting for next six

Sl. No.	Service Area	Expected Service Level	Penalty
		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 C-SOC SLAs, status of operations, key threats and new threats identified, issues and challenges etc.	years to be conducted on the 5th (tentatively) of each month during the operations phase. <u>Penalty:</u> A delay of more than three days will incur a penalty of 1% of C-SOC operations cost for that month.
7	Anti-phishing & Anti-Rogue Mobile application Service along with take down	This service to be provided on a 24/7 basis. Incidents need to be logged and the resolution SLA is as per the incident resolution section.	- Take down of malicious sites/apps within 24 hours of identification and confirmation by the Bank - Daily report of new phishing sites , action taken , instances of reactivation etc. to be shared with Bank <u>Penalty:</u> - For a delay of 4 hours beyond 24 hours after identification in takedown of such sites a penalty of 0.5 % - For a delay of more than one week beyond 24 hours after identification in takedown of such sites a penalty of 2% - For more than one month delay in takedown of such site a penalty of 5% per site
8	Security Device Management and Administration	Bidder is expected to provide this service 24/7 basis. Management and administration of all existing and in-scope security devices / solutions	<u>Penalty:</u> - For more than 1 hour delay (after the Banks confirmation) for rule modification in any of the security devices / solutions will incur a penalty of 1% of monthly C-SOC operations cost per instance. - For wrong rule modification in any of the security solutions will incur a penalty of 10% of the monthly operational 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 50% of monthly operations

Sl. No.	Service Area	Expected Service Level	Penalty
			cost per instance.
9	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.	<u>Penalty:</u> Bidder failing to respond back with details of dashboard/report availability shall be penalty of 5% of the C-SOC monthly operations charges.
10	Proactive monitoring against any security incident/breach	Bidder is expected to proactively monitor Bank's network to defend against any cyber incident/breach	<u>Penalty:</u> 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): • Lack of proactive monitoring • Improper configuration of in-scope devices • 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. The penalty will be restricted to the yearly payout value.

2.4.3 PENALTY

- The Bank expects the Bidder to complete the scope of the project as mentioned in section 2 - scope of work of this document within the timeframe specified in Section 1.4 Project Timelines of this document. Inability of the Bidder either to provide the requirements as per the scope or to meet the timelines as specified would be treated as breach of contract and would invoke the penalty clause. The proposed rate of penalty would be 1% of the value of the affected service or product per week or part there of delay or non-compliance subject to an upper limit of 10% of value of affected service or product & shall be a maximum of 10% of the total cost of that solution from the finalized Bidder for the Bank.

- For example, if the Bidder is not able to supply network equipment at DC or the supplied network solution requires some more parts for its functioning, then the penalty levied will be 1% of the cost of “That Security solution” per week or part there of delay.
- Inability of the Bidder to provide services at the service levels defined would result in breach of contract and would invoke the penalty clause as mentioned in Section 2.3 – Service Levels.
- Notwithstanding anything contained above, no such penalty will be chargeable on the Bidder for the inability occasioned, if such inability is due to reasons entirely attributable to the Bank
- Notwithstanding what is mentioned hereinabove or anywhere else in the tender, the maximum amount that may be levied by way of penalty shall on no account exceed 10 % of the Total Contract value and the contract value will be determined at the time of contract finalization.

2.4.4 RESPONSIBILITY MATRIX

The following table describes the responsibilities of the Bidder, Bank/ consultant 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.

Sl. No.	Activity	Bank / Consultant	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	SOC Operations – Ongoing	S	P	-
5	SOC Operations Review –Biannual) / Incident based Audit	S	-	P
6	SLA Reports	S	P	-
7	Incident Management	S	P	P
“V” - Validated (Responsible for Validating the activity) “P” - Performed (Primary responsibility for executing the activity) “S” – Signed Off (Responsible for providing the go-ahead) “M”- Monitoring (Responsible for continuous monitoring of activity)				

2.4.5 TABLES OF INCIDENT MATRIX

Incident to be Reported within (If unresolved)	Escalation Hierarchy

3. TERMS AND CONDITIONS

3.1 GENERAL

Central Bank of India invites the Bidder's attention to the following terms and conditions which underlines this RFP and which provide a statement of understanding between the interested parties.

The Bank expects the Bidder to adhere to the terms of this RFP and would not accept any deviations to the same. If the Bidder has genuine issues only then should it may provide the nature of non-compliance to the same in the format provided. The Bank reserves its right to not accept such deviations to the tender terms. Refer Appendix 2 Form A 02 - Comments on T&C.

The Bank expects that the Bidder appointed under the RFP shall have the single point responsibility for fulfilling all obligations and providing all supply and delivery of equipment required for the project implementation.

Unless agreed to specifically by the Bank in writing for any changes to the RFP issued, the Bidder's response would not be incorporated automatically in the RFP.

Unless expressly overridden by the specific agreement to be entered into between the Bank and the Bidder, the RFP shall be the governing document for arrangement between the Bank and the Bidder.

3.1.1 TWO BID SYSTEM

Separate Sealed Envelopes Containing Technical Proposal (Technical Bid) and Commercial Proposals (Commercial Bid) should be clearly super scribed as "Technical Bid – RFP for supply, Installation and Maintenance of security solutions" and "Commercial Bid – RFP for supply, Installation and Maintenance of security solutions" respectively and should be addressed to and submitted at: -

Chief Manager, Central Bank of India,
1st Floor, Plot No. 26, Sector – 11
CBD Belapur, Navi Mumbai – 400 614

One hard copy and one soft copy on compact disk, of the Technical Bid and One Hard Copy of the Commercial Bid must be submitted at the same time, giving full particulars in separate sealed envelopes at the Bank's address given below on or before the schedule given above. All envelopes should be securely sealed and stamped. The sealed envelope containing Commercial Bid must be submitted separately to the Bank.

All the envelopes must be super scribed with the following information –

- Type of Offer- (Technical Bid, Commercial Bid) RFP for supply, Installation and Maintenance of security solutions
- Tender Reference Number
- Due Date
- Name of Bidder
- Name of the Authorized Person

All schedules, Formats and Annexure should be stamped and signed by an authorized official of the Bidders Company. The Bidder will also submit copy of the RFP duly stamped and signed on each page by the authorized official of the Bidders Company.

Envelope – I (Technical Bid)

The Technical bid should be complete in all respects and contain all information asked for except prices. The TECHNICAL BID should include all items mentioned in the below list.

- “Bidders Information” format along with supporting documents.
- The Bidder will have to give presentation on the following points as a part of the technical evaluation.
 - ✓ Proposed solution
 - ✓ Provide rationale for model and analytical capabilities of the model selected.
 - ✓ Method and timeline for implementation
 - ✓ Implementation of suggested methodology
 - ✓ Deliverables
 - ✓ Project plan
 - ✓ Proposed team details such as qualifications, experience etc.
 - ✓ Case study of any of the similar audits carried out in the past
 - ✓ Certificate of the public sector Bank as a proof for implementation

The Technical bid should not contain any price information. The TECHNICAL BID should be complete to indicate that all products and services asked for are quoted and should give all required information. A Xerox copy of original commercial offer with prices duly masked be submitted along with the Technical Bid.

Envelop- II (Commercial Bid)

The Commercial bid should give all relevant price information and should not contradict the TECHNICAL BID in any manner. A hard copy of the Commercial Bid duly masking the prices be submitted along with the Technical Bid.

The prices quoted in the commercial bid should be without any conditions. The Bidder should submit an undertaking that there are no deviations to the specifications mentioned in the RFP either with the technical or commercial bids submitted.

Envelope III (EMD Amount)

This envelope should contain the demand draft / Bank Guarantee for Rs.2,00,00,000/- (Two Crore only) towards EMD favoring “Central Bank of India payable at Mumbai.

These three envelopes containing the Technical bids, Commercial bid and EMD amount should be separately submitted. Please note that any envelope containing both technical and commercial bid will be rejected. However, all the three separate envelopes should be submitted in a single large envelope:

- All the covers thus prepared should indicate clearly the Name and Address of the Bidder.
- The Bidder shall bear all the costs associated with the preparation and submission of the bid and Central Bank of India will in no case be responsible or liable for those costs, regardless of the conduct or the outcome of the tendering process.
- Bids submitted without EMD and Application Fee Demand Draft will not be considered for evaluation.
- Bids sent by fax or e-mail will not be considered for evaluation.

3.1.2 DATE OF SUBMISSION

The proposal should be prepared in English and should reach the Bank on or before date and time mentioned above. The proposals received later than the above scheduled date and time will not be accepted. The e-mail address and phone/fax numbers of the Bidder should also be indicated on the sealed cover. The details in both the Bids should be exactly as stipulated and otherwise the offer is liable to be rejected.

3.1.3 LIABILITIES OF BANK

This RFP is not an offer by Bank, but an invitation for Bidder responses. No contractual obligation on behalf of Bank whatsoever shall arise from the RFP process unless and until a formal contract is signed and executed by duly authorized officials of Bank and the Bidder(s).

3.1.4 PROPOSAL PROCESS MANAGEMENT

Bank reserves the right to accept or reject any and all proposals, to revise the RFP, to request one or more re-submissions or clarifications from one or more Bidders, or to cancel the process in part or whole. No Bidder is obligated to respond to or to continue to respond to the RFP. Additionally, Bank reserves the right to alter the requirements, in part or whole, during the RFP process, and without re-issuing the RFP. Each party shall be entirely responsible for its own costs and expenses that are incurred while participating in the RFP and subsequent presentations and contract negotiation processes. Bank has every right to award the contract even if only one Bidder is eligible after technical evaluation.

3.1.5 DATE OF BID EXPIRATION

Proposals must be valid for a minimum of 210 days from the date of technical bid submission. Responses must clearly state the validity of the bid and its explicit expiration date.

3.1.6 BIDDER INDICATION OF AUTHORIZATION TO BID

Responses submitted by a Bidder to this RFP (including response to functional and technical requirements) represent a firm offer to contract on the terms and conditions described in the RFP. The proposal must be signed by an official authorized to sign on behalf of Bidder's firm/company. Bidder must clearly identify the full title and authorization of the designated official and provide a statement of bid commitment with the accompanying signature of the official and submit the copy of power of attorney / authority letter authorizing the signatory to sign the bid.

3.1.7 RFP OWNERSHIP

The RFP and all supporting documentation/templates are the sole property of Central Bank of India and should NOT be redistributed, either in full or in part thereof, without the prior written consent of the Bank. Violation of this would be a breach of trust and may, inter-alia cause the Bidder to be irrevocably disqualified. The aforementioned material must be returned to Bank when submitting the Bidder proposal or upon request. In case the Bidder is not interested in responding to the RFP, the RFP documents and any appendices must be returned to Bank immediately.

3.1.8 PROPOSAL OWNERSHIP

The proposal and all supporting documentation submitted by the Bidder shall become the property of Central Bank of India unless the Bidder specifically requests, in writing, that the proposal and documentation be returned or destroyed.

3.1.9 BID PRICING INFORMATION

By submitting a signed bid, the Bidder certifies that:

The Bidder has arrived at the prices in its bid without agreement with any other Bidder of this RFP for the purpose of restricting competition. The prices in the bid have not been disclosed and will not be disclosed to any other Bidder of this RFP. No attempt by the Bidder to induce any other Bidder to submit or not to submit a bid for restricting competition has occurred.

3.1.10 BIDDER STATUS

Each Bidder must indicate whether or not they have any actual or potential conflict of interest related to contracting services with Central Bank of India.

3.1.11 CONFIDENTIALITY

The RFP document is confidential and is not to be disclosed, reproduced, transmitted, or made available by the Recipient to any other person. The RFP document is provided to the Recipient on the basis of the undertaking of confidentiality given by the Recipient to Bank. Bank may update or revise the RFP document or any part of it. The Recipient acknowledges that any such revised or amended document is received subject to the same confidentiality undertaking. The Recipient will not disclose or discuss the contents of the RFP document with any officer, employee, consultant, director, agent, or other person associated or affiliated in any way with Bank or any of its customers or suppliers without the prior written consent of Bank.

This tender document contains information proprietary to the Bank. Each recipient is entrusted to maintain its confidentiality. It should be disclosed only to those employees involved in preparing the requested responses. The information contained in the tender document may not be reproduced in whole or in part without the express permission of the Bank. Disclosure of any such sensitive information to parties not involved in the supply of contracted services will be treated as breach of trust and could invite legal action. This will also mean termination of the contract and disqualification of the said Successful Bidder.

Responses received become the property of the Bank and cannot be returned. Information provided by each Bidder will be held in confidence, and will be used for the sole purpose of evaluating a potential business relationship with the successful Bidder.

“Confidential Information” means any and all information that is or has been received by the successful Bidder (“Receiving Party”) from the Bank (“Disclosing Party”) and that:

- Relates to the Disclosing Party; and as designated by the Disclosing Party as being confidential or is disclosed in circumstances where the Receiving Party would reasonably understand that the disclosed information would be confidential or
- Is prepared or performed by or on behalf of the Disclosing Party by its employees, officers, directors, agents, representatives or consultants.
- Without limiting the generality of the foregoing, Confidential Information shall mean and include any information, data, analysis, compilations, notes, extracts, materials, reports, drawings, designs, specifications, graphs, layouts, plans, charts, studies, memoranda or other documents, or materials that may be shared by the Bank with the Bidder.
- “Confidential Materials” shall mean all tangible materials containing Confidential Information, including, without limitation, written or printed documents and computer disks or tapes, whether machine or user readable.
- Information disclosed pursuant to this clause will be subject to confidentiality for the term of contract plus two years.
- The Receiving Party shall, at all times regard, preserve, maintain and keep as secret and confidential all Confidential Information and Confidential Materials of the Disclosing Party howsoever obtained and agrees that it shall not, without obtaining the written consent of the Disclosing Party:
- Unless otherwise agreed herein, use any such Confidential Information and materials for its own benefit or the benefit of others or do anything prejudicial to the interests of the Disclosing Party or its customers or their projects.

In maintaining confidentiality hereunder the Receiving Party on receiving the confidential information and materials agrees and warrants that it shall:

- Take at least the same degree of care in safeguarding such Confidential Information and materials as it takes for its own confidential information of like importance and such degree of care shall be at least, that which is reasonably calculated to prevent such inadvertent disclosure;
- Keep the Confidential Information and Confidential Materials and any copies thereof secure and in such a way so as to prevent unauthorized access by any third party;
- Limit access to such Confidential Information and materials to those of its directors, partners, advisers, agents or employees, sub-contractors and contractors who are directly involved in the consideration/evaluation of the Confidential Information and bind each of its directors, partners, advisers, agents or employees, sub-contractors and contractors so involved to protect the Confidential Information and materials in the manner prescribed in this document; and upon discovery of any unauthorized disclosure or suspected unauthorized disclosure of Confidential Information, promptly inform the Disclosing Party of such disclosure in writing and immediately return to the Disclosing Party all such Information and materials, in whatsoever form, including any and all copies thereof.

- The Receiving Party who receives the confidential information and materials agrees that on receipt of a written demand from the Disclosing Party:
 - ✓ Immediately return all written Confidential Information, Confidential materials and all copies thereof provided to, or produced by it or its advisers, as the case may be, which is in Receiving Party's possession or under its custody and control;
 - ✓ To the extent practicable, immediately destroy all analyses, compilations, notes, studies, memoranda or other documents prepared by it or its advisers to the extent that the same contain, reflect or derive from Confidential Information relating to the Disclosing Party;
 - ✓ So far as it is practicable to do so immediately expunge any Confidential Information relating to the Disclosing Party or its projects from any computer, word processor or other device in its possession or under its custody and control; and
 - ✓ To the extent practicable, immediately furnish a certificate signed by its director or other responsible representative confirming that to the best of his/her knowledge, information and belief, having made all proper enquiries the requirements of this paragraph have been fully complied with.
- The restrictions in the preceding clause shall not apply to:
 - ✓ Any information that is publicly available at the time of its disclosure or becomes publicly available following disclosure (other than as a result of disclosure by the Disclosing Party contrary to the terms of this document); or any information which is independently developed by the Receiving Party or acquired from a third party to the extent it is acquired with the valid right to disclose the same.
 - ✓ Any disclosure required by law or by any court of competent jurisdiction, the rules and regulations of any recognized stock exchange or any enquiry or investigation by any governmental, statutory or regulatory body which is lawfully entitled to require any such disclosure provided that, so far as it is lawful and practical to do so prior to such disclosure, the Receiving Party shall promptly notify the Disclosing Party of such requirement with a view to providing the Disclosing Party an opportunity to obtain a protective order or to contest the disclosure or otherwise agree to the timing and content of such disclosure.
 - ✓ The Confidential Information and materials and all copies thereof, in whatsoever form shall at all times remain the property of the Disclosing Party and its disclosure hereunder shall not confer on the Receiving Party any rights whatsoever beyond those contained in this document.
 - ✓ The confidentiality obligations shall survive the expiry or termination of the agreement between the SI and the Bank.

3.1.12 DISCLAIMER

The Bank and/or its officers, employees disown all liabilities or claims arising out of any loss or damage, whether foreseeable or not, suffered by any person acting on or refraining from acting because of any information including statements, information, forecasts, estimates or projections contained in this document or conduct ancillary to it whether or not the loss or damage arises in connection with any omission, negligence, default, lack of care or misrepresentation on the part of Bank and/or any of its officers, employees.

The short-listed Bidder should execute (a) a Service Level Agreement, 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 (b) Non-disclosure Agreement.

3.1.13 RIGHT TO REJECT

Central Bank of India reserves the right to reject any or all proposals received in response to the RFP without assigning any reasons thereof. Bank reserves the right to waive or modify any formalities, irregularities, or inconsistencies in the bid, which does not prejudice or affect the relative ranking of any Bidder, which shall be binding on all Bidders.

3.1.14 BID SECURITY

- The Bidder shall furnish, as part of its Technical bid, bid security of an amount of Rs.2,00,00,000/- (Rupees Two Crore Only). The bid security is required to protect the Bank against the risk of Bidder's conduct.
- The bid security shall be denominated in the INDIAN RUPEES only and shall be in the form of a Demand Draft / BG favoring "Central Bank of India" by a Scheduled Commercial Bank located in India in the form provided in Appendix 2 Form A 05 of this RFP Any bid not secured in accordance with the above will be rejected by the Bank as non-responsive.
- Unsuccessful Bidders' bid security will be discharged/returned as promptly as possible but not later than 30 days after the expiration of the period of bid validity prescribed by the Bank.
- The successful Bidder's bid security will be discharged upon the Bidder signing the Contract and furnishing the performance guarantee.

✓ The bid security may be forfeited:

- If Bidder withdraws its bid during the period of bid validity specified by the Bidder on the Bid Form;
- Or
- In case of the successful Bidder, if the Bidder fails:
 - ✓ To sign the Contract And
 - ✓ To furnish performance security.
- Period of Validity of Bids: The process of bid evaluation, approval and the subsequent activities may be assumed to take a reasonable amount of time. Therefore, the bids shall remain valid for 210 days after the date of Commercial Bid submission, prescribed by the Bank. A bid valid for a shorter period shall be rejected by the Bank as non-responsive.

3.2 TERMS OF REFERENCE (TOR)

3.2.1 OWNERSHIPS, 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.

3.2.2 ACCEPTANCE TESTING

The Bank will carry out the acceptance tests for testing of related software, security and server virtualization equipment to verify that the supplied equipment & software are as per the Bill of materials. The Bidder shall assist the Bank in all acceptance tests to be carried out by the Bank.

The Bidder shall submit the acceptance test plan as part of their response to the tender enquiry. Post award of the contract a detailed acceptance plan will be created within the framework of the RFP terms. The scope of acceptance test plan would be mutually discussed and agreed upon between Bidder & the Bank. The Bidder shall arrange for the tests at the relevant sites in the presence of the officials of the Bank and / or its consultants. The Bidder should ensure that the tests will involve trouble-free operation of the complete system apart from physical verification and testing and that there shall not be any additional charges payable by the Bank for carrying out this acceptance test.

In case of any discrepancy in the hardware & related software supplied, the Bank reserves the right to terminate the entire agreement in case the Bidder does not rectify or replace the supplied hardware/software and the Bidder shall take back Bidder equipment at Bidder costs and risks. The Bidder shall ensure that all costs associated with insurance from the date of transfer of title until the final acceptance by the Bank will be borne by the Bidder and the asset insured in the name of the Bank. The Bidder shall provide the insurance certificates for insurance of the 'Bidder Supplied Equipment' to the Bank along with supply of Equipment.

The installation cum acceptance test will be deemed to be fully and finally accepted by the Bank in the event the Bank has not completed and communicated the results of the acceptance tests to the Bidder within 20 days of submission of all documents duly accepted by the various locations of the Bank to the head office. The Installation cum Acceptance Test and Check certificates jointly signed by representative of the Bidder and official or any consultant / auditor appointed by the Bank will be received at Head Office of the Bank along with Bidder invoice for scrutiny before taking up the request for consideration of payment.

In all cases, the Bidder shall have the sole responsibility for bearing all additional charges, costs or expenses incurred in correcting, reworking or repairing the defective or non-conforming hardware/software, unless such failure is due to reasons entirely attributable to the Bank.

At the discretion of Central Bank of India, acceptance tests will be conducted by the Bidder at the site of installation in the presence of the officials of Central Bank of India and/ or its nominated consultants. There shall not be any additional charges payable by central Bank of India for carrying out this acceptance test. Central Bank of India will take over the system on successful completion of the above acceptance.

3.2.3 COMPLIANCE WITH LAWS

Compliance with all applicable laws: The Bidder shall undertake to observe, adhere to, abide by, comply with and notify 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 tender and shall indemnify, keep indemnified, hold harmless, defend and protect the Bank and its employees/officers/staff/ personnel/representatives/agents from any failure or omission on its part to do so and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from.

Compliance in obtaining approvals/permissions/licenses: The 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, and in the event of any failure or omission to do so, shall indemnify, keep indemnified, hold harmless, defend, protect and fully compensate the Bank and its employees/ officers/ staff/ personnel/ representatives/agents from and against all claims or demands of liability and all consequences that may occur or arise from any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from and the Bank will give notice of any such claim or demand of liability within reasonable time to the Bidder.

All necessary compliances relating to the transaction such as disclosure in the returns to be filed, Tax collected at Source (if applicable) etc. shall be duly undertaken by the supplier/ Bidder and in case of any non-compliance or delayed compliance, the Bank shall have the right to recover interest and/ or penalty that may be levied including liquidated damages up to 10% of the value of supplier.

This indemnification is only a remedy for the Bank. The Bidder is not absolved from its responsibility of complying with the statutory obligations as specified above.

Indemnity would be limited to court awarded damages and shall exclude indirect, consequential and incidental damages. However, indemnity would cover damages, loss or liabilities suffered by the Bank arising out of claims made by its customers and/or regulatory authorities.

3.2.4 ASSIGNMENT

Bank may assign the hardware and related software provided therein by the 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 AMC services to any of the sub-contractors, at its sole option, upon the occurrence of any of the following: (i) Bidder refuses to perform; (ii) Bidder is unable to perform; (iii) Termination of the contract with the 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 the Bidder. The Bidder shall ensure that the said subcontractors shall agree to provide such services to the Bank at no less favorable terms than those provided by the Bidder and shall include appropriate wordings to this effect in the agreement entered into by the Bidder with such sub-contractors. The assignment envisaged in this scenario is only in certain extreme events such as refusal or inability of the Bidder to perform or termination/expiry of the contract.

3.2.5 INSURANCE

In addition to the insurance policies taken by the Bidder with respect to the transportation of the equipment as set out above, the Bidder shall maintain adequate professional liability and an all risk Insurance for the aggregate of all deliverables and services to be rendered by virtue of Hardware Up gradation Project and shall provide to the Bank on request copies of such policy of insurance and evidence that the premiums have been paid. The Bidder shall procure appropriate insurance policies of the limits acceptable to the Bank for damage to Banks premises, Banks property, data or loss of life, which may occur as a result of or in the course of performing the Bidder's obligations under the RFP. The Bidder also warrants and represents that it shall keep all their respective directors, partners, advisers, agents, representatives and or employees adequately insured in respect of business travel in India and further agrees to provide to the Bank on request copies of such policy of insurance and evidence that the premiums have been paid.

The Bidder shall furnish to the Bank prior to the commencement of the supply of security and server virtualization equipment, copies of the certificates of insurance as stipulated as set out herein certifying that the policies of insurance, endorsed as required, are in full force and effect (together with any required waivers of subrogation). The Bidder shall ensure that the policies contain provision that the Bank will be given thirty (30) days' prior written notice by the insurers in the event of either cancellation or material change in coverage; and that the Bank shall be given thirty (30) days' notice prior to termination of the insurance for failure to renew or pay premium. The Insurance procured by the Bidder shall be primary to any other insurance available to the Bank, its assigns, officers, directors, agents and employees.

The Bidder's obligation to maintain insurance coverage hereunder shall be in addition to, and not in lieu of, the Bidder's other obligations, and the Bidder's liability to the Bank shall not be limited to the amount of coverage. It is usual for Bidders to have name of their customers endorsed as additional insured / beneficiary and provide a copy of the policy to the customers.

The Bank should be added as a "Beneficiary or additional insured" and appropriate certification should be provided by the Bidder's insurer certifying compliance with the provisions of this clause.

The equipment (hardware, software etc.) supplied under the contract shall be fully insured by the successful Bidder against loss or damage incidental to manufacture or acquisition, transportation, storage, delivery and installation. The insurance shall be obtained by the Bidder naming Central Bank of India as the beneficiary, for an amount Equal to 100% of the invoiced value of the goods on "all risks" basis. The period of insurance shall be up to the date the supplied components are accepted and the all rights of the property are transferred to the Bank in the Bank's premises.

Should any loss or damage occur, the selected Bidder shall: -

- Initiate and pursue claim till settlement and
- Promptly make arrangements for repair and / or replacement of any damaged item irrespective of settlement of claim by the underwriters.

Privacy and security safeguards

- 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.
- The Bidder hereby agrees and confirms that they will disclose, forthwith, instances of security breaches.

The Bidder hereby agrees that they will preserve the documents after prior written permission of the Bank.

3.2.6 ORDER CANCELLATION

- The Bank reserves its right to cancel the order in the event of one or more of the following situations, Delays in delivery beyond the specified period for delivery.
- Serious discrepancy in hardware noticed during the pre-dispatch factory inspection or during Installation.

In addition to the cancellation of purchase order, Central Bank of India reserves the right to appropriate the damages by foreclosing the Bank guarantee given by the supplier against the advance payment.

3.2.7 INDEMNITY

Bidder shall indemnify, protect and save the Bank and hold the Bank harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings, (including reasonable attorney fees), relating to or resulting directly or indirectly from (i) an act or omission of the Bidder, its employees, its agents, or employees of the consortium in the performance of the services provided by this contract, (ii) breach of any of the terms of this RFP or breach of any representation or warranty by the Bidder, (iii) use of the deliverables and or services provided by the Bidder, (iv) infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided to fulfill the scope of this project. Bidder shall further indemnify the Bank against any loss or damage to the Bank's premises or property, Bank's data, loss of life, etc., due to the acts of the Bidder's employees or representatives. The Bidder shall further indemnify the Bank against any loss or damage arising out of loss of data, claims of infringement of third-party copyright, patents, or other intellectual property, and third-party claims on the Bank for malfunctioning of the equipment or software or deliverables at all points of time, 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 unless and until justified by authority of the Bank or 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 and users) rights, interest and reputation.

Bidder shall be responsible for any loss of data, loss of life, etc., due to acts of Bidder's representatives, and not just arising out of gross negligence or misconduct, etc., as such liabilities pose significant risk.

Bidder should take full responsibility for its and its employee's actions. Further, since the Bank's data could be integrated/used under Bidder provided software and since the Bidder would be managing the data center, the Bidder should be responsible for loss/compromise or damage to Bank's data.

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.

The Bidder's should indemnify the Bank (including its employees, directors or representatives) from and against claims, losses, and liabilities arising from:

- Non-compliance of the Bidder with Laws / Governmental Requirements
- IP infringement
- Negligence and misconduct of the Bidder, its employees, and agents
- Breach of any terms of RFP, Representation or Warranty
- Act or omission in performance of service.

Indemnity would be limited to court awarded damages and shall exclude indirect, consequential and incidental damages. However indemnity would cover damages, loss or liabilities suffered by the Bank arising out of claims made by its customers and/or regulatory authorities.

The Bidder shall not indemnify the Bank for

- Any loss of profits, revenue, contracts, or anticipated savings or
- Any consequential or indirect loss or damage however caused, provided that the claims against customers and users of the Bank would be considered as a "direct" claim

3.2.8 PUBLICITY

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

3.2.9 SOLICITATION OF EMPLOYEES

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

other party.

3.2.10 INFORMATION OWNERSHIP

All information processed, stored, or transmitted by Bidder equipment belongs to the Bank. By having the responsibility to maintain the equipment, the Bidder does not acquire implicit access rights to the information or rights to redistribute the information. The Bidder understands that civil, criminal, or administrative penalties may apply for failure to protect information appropriately.

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.

3.2.11 CONFIDENTIALITY

"Confidential Information" means any and all information that is or has been received by the Bidder ("Receiving Party") from the Bank ("Disclosing Party") and that:

Relates to the Disclosing Party; and is designated by the Disclosing Party as being confidential or is disclosed in circumstances where the Receiving Party would reasonably understand that the disclosed information would be confidential or is prepared or performed by or on behalf of the Disclosing Party by its employees, officers, directors, agents, representatives or consultants.

Without limiting the generality of the foregoing, Confidential Information shall mean and include any information, data, analysis, compilations, notes, extracts, materials, reports, drawings, designs, specifications, graphs, layouts, plans, charts, studies, memoranda or other documents, or materials relating to the licensed software, the modules, the program documentation, the source codes, the object codes and all enhancements and updates, services, systems processes, ideas, concepts, formulas, methods, know how, trade secrets, designs, research, inventions, techniques, processes, algorithms, schematics, testing procedures, software design and architecture, computer code, internal documentation, design and function specifications, product requirements, problem reports, analysis and performance information, business affairs, projects, technology, finances (including revenue projections, cost summaries, pricing formula), clientele, markets, marketing and sales programs, client and customer data, appraisal mechanisms, planning processes etc. or any existing or future plans, forecasts or strategies in respect thereof.

“Confidential Materials” shall mean all tangible materials containing Confidential Information, including, without limitation, written or printed documents and computer disks or tapes, whether machine or user readable.

Information disclosed pursuant to this clause will be subject to confidentiality for the term of contract plus two years.

Nothing contained in this clause shall limit Bidder from providing similar services to any third parties or reusing the skills, know-how and experience gained by the employees in providing the services contemplated under this clause, provided further that the Bidder shall at no point use the Bank’s confidential information or Intellectual property. The Receiving Party shall, at all times regard, preserve, maintain and keep as secret and confidential all Confidential Information and Confidential Materials of the Disclosing Party howsoever obtained and agrees that it shall not, without obtaining the written consent of the Disclosing Party:

- Disclose, transmit, reproduce or make available any such Confidential Information and materials to any person, firm, Company or any other entity other than its directors, partners, advisers, agents or employees, sub-contractors and contractors who need to know the same for the purposes of maintaining and supporting the Software provided as a part of Hardware expansion Project. The Receiving Party shall be responsible for ensuring that the usage and confidentiality by its directors, partners, advisers, agents or employees, sub-contractors and contractors is in accordance with the terms and conditions and requirements of this tender; or
- Unless otherwise agreed herein, use any such Confidential Information and materials for its own benefit or the benefit of others or do anything prejudicial to the interests of the Disclosing Party or its customers or their projects.
- In maintaining confidentiality hereunder the Receiving Party on receiving the confidential information and materials agrees and warrants that it shall:
 - ✓ Take at least the same degree of care in safeguarding such Confidential Information and materials as it takes for its own confidential information of like importance and such degree of care shall be at least, that which is reasonably calculated to prevent such inadvertent disclosure;
 - ✓ Keep the Confidential Information and Confidential Materials and any copies thereof secure and in such a way so as to prevent unauthorized access by any third party;
 - ✓ Limit access to such Confidential Information and materials to those of its directors, partners, advisers, agents or employees, sub-contractors and contractors who are directly involved in the consideration/evaluation of the Confidential Information and bind each of its directors, partners, advisers, agents or employees, sub-contractors and contractors so involved to protect the Confidential Information and materials in the manner prescribed in this document; and
 - ✓ Upon discovery of any unauthorized disclosure or suspected unauthorized disclosure of Confidential Information, promptly inform the Disclosing Party of such disclosure in writing and immediately return to the Disclosing Party all such Information and materials, in whatsoever form, including any and all copies thereof.

- The Receiving Party who receives the confidential information and materials agrees that on receipt of a written demand from the Disclosing Party:
 - ✓ Immediately return all written Confidential Information, Confidential materials and all copies thereof provided to, or produced by it or its advisers, as the case may be, which is in Receiving Party's possession or under its custody and control;
 - ✓ To the extent practicable, immediately destroy all analyses, compilations, notes, studies, memoranda or other documents prepared by it or its advisers to the extent that the same contain, reflect or derive from Confidential Information relating to the Disclosing Party;
 - ✓ So far as it is practicable to do so immediately expunge any Confidential Information relating to the Disclosing Party or its projects from any computer, word processor or other device in its possession or under its custody and control; and
 - ✓ To the extent practicable, immediately furnish a certificate signed by its director or other responsible representative confirming that to the best of his/her knowledge, information and belief, having made all proper enquiries the requirements of this paragraph have been fully complied with.
- The restrictions in the preceding clause shall not apply to:
 - ✓ Any information that is publicly available at the time of its disclosure or becomes publicly available following disclosure (other than as a result of disclosure by the Disclosing Party contrary to the terms of this document); or any information which is independently developed by the Receiving Party or acquired from a third party to the extent it is acquired with the valid right to disclose the same.
 - ✓ Any disclosure required by law or by any court of competent jurisdiction, the rules and regulations of any recognized stock exchange or any enquiry or investigation by any governmental, statutory or regulatory body which is lawfully entitled to require any such disclosure provided that, so far as it is lawful and practical to do so prior to such disclosure, the Receiving Party shall promptly notify the Disclosing Party of such requirement with a view to providing the Disclosing Party an opportunity to obtain a protective order or to contest the disclosure or otherwise agree to the timing and content of such disclosure.
 - ✓ The Confidential Information and materials and all copies thereof, in whatsoever form shall at all times remain the property of the Disclosing Party and its disclosure hereunder shall not confer on the Receiving Party any rights whatsoever beyond those contained in this document.
 - ✓ The confidentiality obligations shall survive the expiry or termination of the agreement between the Bidder and the Bank. The receiving party shall execute the NDA (Non-Disclosure Agreement) as per attached format.

3.2.12 TECHNOLOGICAL ADVANCEMENTS

The Bidder has to ensure that the equipment supplied are not declared as end of sale for at least 24 months from the date of the submission of the offer. The Bidder also has to ensure that the equipment supplied, as part of this bid are not declared end of support or service for at least 7 years from the date of the submission of offer. The Bidder agrees that all parts & spares for the equipment would be made available during the period of the contract. It will be the obligation of the Bidder to provide a minimum of 1-year notice before any equipment is to be declared as end

of support or sale.

3.2.13 SUCCESSFUL BIDDER'S LIABILITY

The Successful Bidder's aggregate liability in connection with obligations undertaken as a part of the RFP 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 Successful Bidder's liability in case of claims against the Bank resulting from misconduct or gross negligence of the Successful Bidder, its employees and subcontractors or from infringement of patents, trademarks, copyrights or such other Intellectual Property Rights or breach of confidentiality obligations shall be unlimited.

The Bank shall not be held liable for and is absolved of any responsibility or claim/litigation arising out of the use of any third party software or modules supplied by the Bidder as part of this RFP. In no event shall either party be liable for any indirect and incidental or consequential damages or liability, under or in connection with or arising out of this tender or subsequent agreement or the hardware or the software delivered hereunder, howsoever such liability may arise, provided that the claims against customers and users of the Bank would be considered as a direct claim.

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.

3.2.14 GUARANTEES

Bidder should guarantee that the software and allied components used to service the Bank are licensed and legal and the application/ software is free from embedded malicious/ fraudulent code. Confirmation/ Undertaking should be submitted to this effect. All hardware and related software must be supplied with their original and complete printed documentation.

3.2.15 FORCE MAJEURE

- The Bidder shall not be liable for forfeiture of its performance security, liquidated damages or termination for default, if any to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure.
- For purposes of this Clause, "Force Majeure" means an event explicitly beyond the reasonable control of the Bidder and not involving the Bidder's fault or negligence and not foreseeable. Such events may include, Acts of God or of public enemy, acts of Government of India in their sovereign capacity and acts of war.
- If a Force Majeure situation arises, the Bidder shall promptly notify the Bank in writing of such conditions and the cause thereof within fifteen calendar days. Unless otherwise directed by the Bank in writing, the Bidder shall continue to perform Bidder's obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.
- In such a case, the time for performance shall be extended by a period (s) not less than duration of such delay. If the duration of delay continues beyond a period of three

months, the Bank and the Bidder shall hold consultations in an endeavor to find a solution to the problem. Notwithstanding the above the decision of the Bank shall be final and binding on the Bidder.

3.2.16 RESOLUTION OF DISPUTES AND REMEDIES

- The Bank and the successful Bidder shall make every effort to resolve amicably, by direct informal negotiation between the respective project directors of the Bank and the successful Bidder, any disagreement or dispute arising between them under or in connection with the contract.
- If the Bank project director and successful Bidder project director are unable to resolve the dispute after thirty days from the commencement of such informal negotiations, they shall immediately escalate the dispute to the senior authorized personnel designated by the Bidder and Bank respectively.
- If after thirty days from the commencement of such negotiations between the senior authorized personnel designated by the Bidder and Bank, the Bank and the successful Bidder have been unable to resolve amicably a contract dispute; either party may require that the dispute be referred for resolution through formal arbitration.
- All questions, disputes or differences arising under and out of, or in connection with the contract or carrying out of the work whether during the progress of the work or after the completion and whether before or after the determination, abandonment or breach of the contract shall be referred to arbitration by a sole Arbitrator: acceptable to both parties OR the number of arbitrators shall be three, with each side to the dispute being entitled to appoint one arbitrator. The two arbitrators appointed by the parties shall appoint a third arbitrator shall act as the chairman of the proceedings. The award of the Arbitrator shall be final and binding on the parties. The Arbitration and Reconciliation Act 1996 or any statutory modification thereof shall apply to the arbitration proceedings and the venue of the arbitration shall be Mumbai.
- 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) the expiry of five days after posting if sent by registered post with A.D., or (iii) the business date of receipt, if sent by courier.
- This RFP shall be governed and construed in accordance with the laws of India. The courts of Mumbai alone and no other courts shall be entitled to entertain and try any dispute or matter relating to or arising out of this RFP. Notwithstanding the above, the Bank shall have the right to initiate appropriate proceedings before any court of appropriate jurisdiction, should it find it expedient to do so.
- Notwithstanding the existence of the a dispute and/or commencement of arbitration proceedings, bidder will be expected to continue the facilities management services 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 satisfactorily as per satisfaction of the Bank.

- The bidder acknowledges that if bidder fails to comply with any of its obligations hereunder, if Bank suffers any or all immediate, irreparable harm for which monetary damages may not be adequate. The bidder agrees that, in addition to all other remedies provided at law or in equity, the Bank shall be entitled to injunctive relief, restraining order, right of recovery, specific performance, or such other equitable relief as a court of competent jurisdiction may deem necessary or appropriate to restrain the vendor from committing any violation or enforce the performance of the covenants, obligations and representation contained in this RFP and subsequent Agreement(including Purchase Order/s). 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.

3.2.17 EXIT OPTION AND CONTRACT RE-NEGOTIATION

- The Bank reserves the right to cancel the contract in the event of happening one or more of the following Conditions:
 - ✓ Failure of the successful Bidder to accept the contract and furnish the Performance Guarantee within 10 days of receipt of purchase contract;
 - ✓ Delay in delivery beyond the specified period;
 - ✓ 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.
- The Bank will reserve a right to re-negotiate the price and terms of the entire contract with the Bidder at more favorable terms in case such terms are offered in the industry at that time for projects of similar and comparable size, scope and quality.
- Notwithstanding the existence of a dispute and/ or the commencement of arbitration proceedings, the successful Bidder should continue to provide services to the Bank as per the contract.

3.2.18 SEVERABILITY

If any of the provisions of this Agreement may be constructed in more than one way, one of which would render the provision illegal or otherwise voidable or unenforceable, such provision shall have the meaning that renders it valid and enforceable.

In the event any court or other government authority shall determine any provisions in this Agreement is not enforceable as written, the Parties agree that the provision shall be amended so that it is enforceable to the fullest extent permissible under the laws and public policies of the jurisdiction in which enforcement is sought, and affords the Parties the same basic rights and obligations and has the same economic effect as prior to amendment.

In the event that any of the provisions of this Agreement shall be found to be void, but would be valid if some part thereof was deleted or the scope, period or area of application were reduced,

then such provision shall apply with the deletion of such words or such reduction of scope, period or area of application as may be required to make such provisions valid and effective; provided however, that on the revocation, removal or diminution of the law or provisions, as the case may be, by virtue of which such provisions contained in this Agreement were limited as provided hereinabove, the original provisions would stand renewed and be effective to their original intent, as if they had not been limited by the law or provisions revoked. Notwithstanding the limitation of this provision by any law for the time being in force, the Parties undertake to, at all times observe and be bound by the spirit of this Agreement.

3.2.19 CORRUPT AND 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.

3.2.20 WAIVER

No failure or delay on the part of either party relating to the exercise of any right power privilege or remedy provided under this RFP or subsequent agreement with the other party shall operate as a waiver of such right power privilege or remedy or as a waiver of any preceding or succeeding breach by the other party nor shall any single or partial exercise of any right power privilege or remedy preclude any other or further exercise of such or any other right power privilege or remedy provided in this RFP all of which are several and cumulative and are not exclusive of each other or of any other rights or remedies otherwise available to either party at law or in equity.

3.2.21 VIOLATION OF TERMS

The Bank clarifies that the Bank shall be entitled to an injunction, restraining order, right for recovery, suit for 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 in this RFP. 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.

3.2.22 TERMINATION

- The Bank shall be entitled to terminate the agreement with the Bidder at any time by giving ninety (90) days prior written notice to the Bidder.
- The Bank shall be entitled to terminate the agreement at any time by giving notice if:
 - ✓ The Bidder breaches its obligations under the RFP or the subsequent agreement and if the breach is not correct within 15 days from the date of notice.
 - ✓ The Bidder (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.

Termination for default

The Bidder shall have right to terminate only in the event of winding up of the Bank

Bank may, without prejudice to any other remedy for breach of agreement, by written notice of default sent to the successful Bidder, terminate the agreement in whole or in part:

- If the successful Bidder fails to deliver any or all of the Goods and Services within the time period(s) specified in the agreement, or within any extension thereof granted by Bank or
- If the successful Bidder fails to perform any other obligation(s) under the agreement.
- If the successful Bidder, in the judgment of Bank is engaged in corrupt or fraudulent practices in competing or for executing the agreement.

In the event Bank terminates the agreement in whole or in part, Bank may procure, upon such terms and in such manner, as it deems appropriate, Goods and services similar to those undelivered and the selected successful Bidder shall be liable to Bank for any excess costs for such similar Goods and/or Services. However, the selected successful Bidder shall continue performance of the agreement to the extent not terminated. The notice period will be minimum 2 (Two) months.

In case the contract is terminated then all undisputed payment will be given to vendor, but disputed payment shall be adjusted by way of penalty from invoices or Performance Bank Guarantee.

Termination for Insolvency

If the Bidder becomes bankrupt or insolvent, has a receiving order issued against it, compounds with its creditors, or, if the Bidder is a corporation, 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 the Bidder takes or suffers any other analogous action in consequence of debt; then the Bank plans to, at any time, terminate the contract by giving written notice to the Bidder. If the contract is terminated by the Bank in terms of this Clause, termination will be without compensation to the Bidder, provided that such termination will not prejudice or affect any right of action or remedy

which has accrued or will accrue thereafter to the Bank. In case, the termination occurs before implementation in all the locations in terms of this clause, the Bank is entitled to make its claim to the extent of the amount already paid by the Bank to the Bidder.

3.2.23 EFFECT OF TERMINATION

- The Bidder agrees that it shall not be relieved of its obligations under the reverse transition mechanism notwithstanding the termination of the assignment.
- 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 and maintenance. The reverse transition will be for the period of 3 (Three) months post the notice period.
- Same terms (including payment terms) which were applicable during the term of the contract should be applicable for reverse transition services
- The Bidder agrees that after completion of the Term or upon earlier termination of the assignment the Bidder shall, if required by the Bank, continue to provide warranty/AMC services to the Bank at no less favorable terms than those contained in this RFP. In case the Bank wants to continue with the Bidder's services after the completion of this contract then the Bidder shall offer the same or better terms to the Bank. Unless mutually agreed, the rates shall remain firm.
- The Bank shall make such prorated payment for services rendered by the Bidder and accepted by the Bank at the sole discretion of the Bank in the event of termination, provided that the Bidder is in compliance with its obligations till such date. However, no payment for "costs incurred, or irrevocably committed to, up to the effective date of such termination" will be admissible. There shall be no termination compensation payable to the Bidder.
- Termination shall not absolve the liability of the Bank to make payments of undisputed amounts to the Bidder for services rendered until the effective date of termination. Termination shall be without prejudice to any other rights or remedies a party may be entitled to hereunder or at law and shall not affect any accrued rights or liabilities or either party nor the coming into force or continuation in force of any provision hereof which is expressly intended to come into force or continue in force on or after such termination.

3.2.24 FORMAT FOR TECHNICAL OFFER

The Technical offer must be made in a structured and neat manner. Brochures/leaflets etc. should not be submitted in loose form.

The suggested format for submission of technical offer is as follows:

- Index
- Covering letter.
- Details of the Bidder.
- Masked Bill of materials. This table should not contain any price information.
- Technical Offer with Specifications, complete with all the columns filled in.
- Block diagram of the solution offered. The block diagram will contain the following information

- ✓ The equipment(s) used in the solution.
- ✓ Different modules used.
- ✓ Cables and other components included in the offer.
- ✓ Interconnection of all the components offered.
- ✓ Full details of the proposed solution in terms of technical capabilities.
- Scheduled date of commencement of delivery and completion of the project
- Project Schedule for completing the work (Delivery and implementation)
- Terms and Conditions Compliance Table in the following format. This table must cover Bidder's response to all the terms and conditions specified in the tender document.

Term No	Short Description of term	Complied (Yes/No)	Detailed explanation about deviation, if not complied
1	Technical evaluation and performance evaluation		
X			

- Warranty details (for all relevant schedules). This should not contain any price information.
- Printed Technical Brochures and data sheets pertaining to different components offered.
- Manufacturer's Authorization Form.
- The support and Maintenance plan for the Bank for the services to be provided during the warranty maintenance period.
- Supporting documents, as asked for in the tender document.
- Valid Bank Draft for EMD.

3.2.25 OTHER GENERAL CONDITIONS

- All responses received after the due date/time would be considered late and would be rejected.
- All responses by the Bidders to this RFP document shall be binding on such Bidders for a period of 210(Two Ten) days after the submission of the bids.
- Any additional or different terms and conditions proposed by the Bidder would be rejected unless expressly assented to in writing by the Bank.
- Bank reserve the absolute right to reject the offer if it is not in accordance with its requirements and no further correspondence, whatsoever, will be entertained by the Bank in the matter.
- Any technical or commercial bid, submitted cannot be withdrawn / modified after the last date for submission of the bids.
- Each offer should specify only a single solution which is cost effective and meet the tender specifications and should not include any alternatives.
- The Bidder shall bear all costs associated with the preparation and submission of its bid, attending pre-bid meeting or arranging Product Walk through and Bank will in no case

be responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

- The Bidder shall also indemnify Bank against all third party claims of Intellectual Property Rights infringement such as Patent, Trademark, Copy Right or industrial design rights arising from use of the goods, software(s), hardware(s) or any part thereof in India and abroad.
- To assist in the scrutiny, evaluation and comparison of offers Bank may, at its discretion, ask some or all Bidders for clarification of their offer. The request for clarification and the response shall be in writing and no change in the price or substance of the bid shall be sought, offered or permitted.
- In the event of any claim asserted by the third party of infringement of copyright, patent, trademark or industrial design rights, arising from the use of the Goods or any part thereof in India, the Bidder shall act expeditiously to extinguish such claims. If the Bidder fails to comply and Bank is required to pay compensation to a third party resulting from such infringement, the Bidder shall be responsible for the compensation including all expenses, court costs and lawyer's fees. Bank will give notice to the Bidder of such claims, if it is made, without delay by fax/email/registered post etc.
- The successful Bidder and Bank should execute:
- ✓ **Service Level Agreement:** This 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.
- ✓ **SLA Schedule is as Refer to Section 2.5**

Bidder shall provide personnel support during warranty period.

Non-Disclosure Agreement as Refer to Appendix 2 Form A 07-Non-Disclosure Agreement.

The successful Bidder should execute the SLA and NDA as per format of the Bank within one month from the date of acceptance of Letter of Appointment.

Integrity Pact – Each participating bidder/s shall submit Integrity Pact as per attached Annexure-13 on duly stamped of INR 500. Integrity pact should submit by all participating bidder at the time of submission of Bid documents or as per satisfaction of the Bank. The Non submission of Integrity Pact as per time scheduled prescribed by Bank may be relevant ground of disqualification to participating in Bid process.

3.2.26 COSTS & CURRENCY PRICE COMPOSITION

The Bidder is expected to quote unit price in Indian Rupees (without decimal places) for all components (hardware, software etc.) 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.

Goods and Services Taxes (GST) and its Compliance-

- 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-
- 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.
- 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.
- If supplier/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.

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 in this RFP. 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.

3.2.27 FIXED PRICE

The commercial offer shall be on a fixed price basis, excluding of taxes. No price variation relating to increases in dollar price variation etc. is permitted.

3.2.28 PROJECT COMPLETION TIME

The Bidder shall be responsible for delivery, installation & commissioning of all the equipment ordered at the site and for making them fully operational at no additional charge within 9 months of receiving the purchase order. The installation should be done in such a way that it does not affect the normal operations of the Bank in any way.

Appropriate insurance to cover the equipment for the transit period and till the time of its acceptance by Central Bank of India at the respective site is to be taken by the Bidder. At the discretion of Central Bank of India, there will be an acceptance test conducted by the Bidder in presence of Central Bank of India officials and/or its nominated consultants after installation of complete equipment. In case of serious discrepancy in hardware/software supplied, Central Bank of India may cancel the entire purchase order and return the equipment back to the Bidder at Bidder's costs and risks.

3.2.29 COMPLETENESS OF INSTALLATION

The installation will be deemed as incomplete if any of the component and other necessary accessories and equipment(s) or any documentation/media is not delivered or is delivered but

not installed and/or not operational or not acceptable to Central Bank Of India after acceptance testing/examination.

In such an event, the supply & installation will be termed as incomplete and it will not be accepted and warranty period will not commence. The entire site will be accepted after complete commissioning of equipment and satisfactory working of the entire equipment for a minimum period of 15(fifteen) days.

3.2.30 LIQUIDATED DAMAGES

The Bank will consider the inability of the Bidder to deliver or install the equipment within the specified time limit, as a breach of contract and would entail the payment of Liquidation Damages on the part of the Bidder. The liquidation damages represent an estimate of the loss or damage that the Bank may have suffered due to delay in performance of the obligations (relating to delivery, installation, Operationalization, implementation, training, acceptance, warranty, maintenance etc. of the equipment(s)) by the Bidder.

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

Non-delivery of any component or other services mentioned in the order Non-delivery of supporting documentation

If the Bidder fails to deliver any or all of the Goods or perform the Services within the time period(s) specified in the Contract, the Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to 1% of the order value of the Device, Software per week or part thereof until actual delivery or performance, (3 days will be treated as a week); and the maximum deduction is 10% of the contract price. 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.

3.2.31 BLACKLISTING

The Bank reserves its right to blacklist to concern Bidder to participate in future tender process, in the event of delay in project beyond the specified period or non-compliance of the RFP terms or non-fulfilment of RFP functional requirements or severe bugs in the application or proposed system performance is not satisfactory. Bank shall have right to exercise power conferred under this clause along with any or all right incorporated in this RFP / Agreement.

3.2.32 HARDWARE WARRANTY

The offer must include a minimum **Three years comprehensive on-site warranty** from the date of installation and acceptance of the system by Central Bank of India. The warranty will start only after acceptance of Installation.

The Bidder has to submit document for back to back agreement with the Hardware OEM (Original Equipment Manufacturer). The Bidder should make proper arrangement with respective OEM to ensure that back to back arrangement in place for continuing support for the entire Project. So that continuity is maintained for project in the event of insolvency, Bankruptcy, liquidation, acquisition, windup, amalgamation or termination on default of Bidder. If the OEM provides login username & password for downloading firmware, other software's then the Bidder has to pass on the same to Bank. Bidder shall be fully responsible for the manufacturer's warranty in respect of quality and workmanship of all equipment, accessories etc. covered by the tender. Bidder must warrant all equipment,

accessories, spare parts etc. against any manufacturing defects during the warranty period. During the warranty period, Bidder shall maintain the systems and repair/replace at the installed site all defective components and upgrade the firmware, at no additional charge to Central Bank of India.

If any of the components are not available or difficult to procure or the procurement is likely to be delayed for replacement if required, the replacement shall be carried out with state of the art technology equipment of equivalent capacity or higher capacity at no additional charges to Central Bank of India.

3.2.33 ANNUAL MAINTENANCE CHARGES

The Bidder shall provide the maintenance (Warranty, AMC & ATS) for a period of five years beginning from the date of acceptance test procedure signoff. The Warranty period for the 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. The Bidder must factor the costs in the Bill of Material accordingly. As part of warranty, AMC & ATS support the Bidder has to:

- Provide support for hardware and software components during the warranty period.
- Provide on-site comprehensive warranty for all the components provided as part of this RFP. The Warranty (ATS/AMC) should be back to back from OEM onsite and comprehensive in nature.
- Warrant all the component and licenses 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 hardware and software.
- Provide for maintenance of Hardware, including preventive Hardware support, as well as repair or replacement activity after a 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. 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 upgrade.
- Provide the support services like repair, replacement to resolve the problem as per the service levels defined in Section 2.5.
- Defective hardware shall be replaced by The Bidder at his own cost, including the cost of transport etc. The Bidder shall not charge The Bank for any extra charges related to this activity.
- Provide adequate spares for the critical components of the hardware within the stipulated time window to ensure call to resolution.
- Provide on-site support whenever required by The Bank. For factoring purposes, the Bidders should factor not more than 8 visits each year for on-site support on specific request from 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 the Bidder during the period of warranty.
- During the Warranty period, the Bidder will have to undertake system maintenance and replacement or repair of defective hardware & storage equipment.

- Upon receipt of such notice the Bidder shall, as mentioned below, repair or replace the defective goods or parts thereof, without any cost to The Bank.
- In case components are taken away for repairs, the Bidder shall provide similar standby components so that the components can be put to use in the absence of the originals/replacements without disrupting the Bank's regular work during holidays and non-business hours with written consent from the Bank.
- If during operation, the down time of any piece of equipment or component thereof does not prove to be within reasonable period, the Supplier 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 tenure of the warranty, shift the goods wholly or in part to other location(s) within the Country and in such case the Supplier 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 warranty services delivered by their appointed Bidder or System Integrator, then the OEM shall transfer such warranty services to that preferred Bidder at no additional cost to The Bank.
- The 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.
- The 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 the Bidder, that may develop under normal use of the supplied Goods in the conditions prevailing at the final destination.
- The Bidder's/OEM'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 Bidders are expected to provide technical and commercial proposals in accordance with the terms and conditions contained herein. Evaluation criteria, evaluation of the responses to the RFP and subsequent selection of the successful Bidder shall be as per the process defined in this RFP. Their decision shall be final and no correspondence about the decision shall be entertained.

Bidder's failure to deliver all required components of a fully functional system (pertaining to the scope of the project) within the stipulated time schedule or by the date extended by the Bank, unless such failure is due to reasons entirely attributable to The Bank, it will be a breach of contract.

3.2.34 FACILITY MANAGEMENT

Facility Management Services would be out of scope of the Bidder.

3.2.35 PERFORMANCE BANK GUARANTEE

The successful Bidder should provide a performance Bank guarantee for the contract period and additional 3 months for an amount equivalent to 10% of the total order value from a

Nationalized / PSU Bank/Scheduled commercial Bank in the format specified by the Bank within 30 days from the date of purchase order. The Proforma for Performance Bank Guarantee is attached as Appendix 2 Form A 06 - Performance Bank Guarantee.

In the event of non-performance of obligation or failure to meet the terms / requirements of the RFP, Bank shall be entitled to invoke the performance Bank guarantee without notice or right of demur to the successful Bidder.

Bank reserves its right to invoke the Performance Bank Guarantee besides cancellation of the entire Purchase Order in the event of breach and/or nonobservance of any of the terms of performance Bank guarantee.

3.2.36 NON-DISCLOSURE AGREEMENT

The successful Bidder will have to sign a Nondisclosure agreement with the Bank as per the format enclosed as annexure.

3.2.37 CANCELLATION OF ORDER

The Bank reserves its right to cancel the Purchase Order at any time i.e. in the event of delay in project beyond the specified period or noncompliance of the RFP terms or nonfulfillment of RFP functional requirements or severe bugs in the application or proposed system performance is not satisfactory etc. In addition to the cancellation of Purchase order, the Bank reserves the right to invoke the Bank Guarantee given by the successful Bidder to recover the damages.

3.2.38 SECURITY

The successful Bidders' proposal must include a plan to safeguard the confidentiality of the Bank's business information, legacy applications and data.

3.2.39 PATENT RIGHTS/ INTELLECTUAL PROPERTY RIGHTS

The Successful Bidder shall ensure that the equipment (including hardware and software) does not infringe third party intellectual property rights. If a third party's claim endangers or disrupts the Bank's use of the software, the Successful Bidder shall be required to, at no further expense, charge, fees or costs to the Bank, (i) obtain a license so that the Bank may continue use of the equipment in accordance with the terms of this Agreement and the license agreement; or (ii) modify the equipment without affecting the functionality in any manner so as to avoid the infringement; or (iii) replace the equipment with a compatible, functionally equivalent and non-infringing product; or (iv) refund to the Bank the amount paid for the infringing software and bear the incremental costs of procuring a functionally equivalent equipment from a third party, provided the option under the sub clause (iv) shall be exercised by the Bank in the event of the failure of the Successful Bidder to provide effective remedy under options (i) to (iii) within a reasonable period which would not affect the normal functioning of the Bank. The Successful Bidder shall have no liability for any claim of infringement based on (i) a claim which continues because of Bank's failure to use a modified or replaced software that is at least functionally equivalent to the software, or the Bank's failure to use corrections, fixes, or enhancements made available and implemented by the Successful Bidder, despite notice of such failure by the Successful Bidder in writing, (ii) any change, not made by or on behalf of the Successful Bidder, to some or all of the software/deliverables supplied by the Successful

Bidder or modification thereof; or (iii) the Bank's continued misuse of some or all of the software/deliverables or any modification thereof despite notice from the Successful Bidder of such misuse in writing.

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 Successful Bidder as part of this Agreement.

3.2.40 AUDIT/ REVIEW/MONITORING/VISITATION

Bank shall undertake a periodic review of service provider 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 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:-

- 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.
- 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.
- 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.
- 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.

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 Vendor'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 without prior approval /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 without prior notice to ensure that data provided by the Bank is not misused. The Vendor shall cooperate with the authorized representative(s) of the Bank and shall provide all information/ documents\required by the Bank.

3.2.41 INDEPENDENT CONTRACTOR

The Bidder shall perform its obligations under this Agreement as an independent contractor, and may engage subcontractors to perform any of the Deliverables or Services, after taking prior approval in writing from the Bank. Neither this Agreement nor the Bidder's performance of obligations under this Agreement shall create an association, partnership, joint venture, or relationship of principal and agent, master and servant, or employer and employee, between the Bank and the Bidder or its employees, subcontractor; and neither Party shall have the right, power or authority (whether expressed or implied) to enter into or assume any duty or obligation on behalf of the other Party. This Agreement does not intent to create, constitute or evidence any partnership, joint venture, trust or employer/employee relationship amongst the Parties and constitutes an agreement between principals. None of the Parties shall be entitled to make, or allow to be made, any representation that any such relationship exists between the Parties. Other than the relationship of sponsor and the consequent inter-se rights and obligations between the Bank, in relation to this Agreement, the right of a Party to act on behalf of the other Party for, or to incur any obligation on behalf of, the other Party, is limited to the manner provided in this Agreement.

The Bidder shall be responsible for managing the activities of its personnel or the personnel of its subcontractors/franchisees/agents and shall be accountable for all of them. The Bidder shall be vicariously liable for any acts, deeds or things done by its/their employees, agents, contractors, subcontractors etc. The Bidder shall be the principal employer of the employees, agents, contractors, subcontractors etc. engaged by Bidder and shall be vicariously liable for all the acts, deeds or things, whether the same is within the scope of power or outside the scope of power, vested under this Agreement. No right of any employment shall accrue or arise, by virtue of engagement of employees, agents, contractors, subcontractors etc. by the Bidder, for any assignment under the Purchase Order issued under this Agreement. All remuneration, claims, wages, dues etc. of such employees, agents, contractors, subcontractors etc. of Bidder shall be paid by Bidder alone and the Bank shall not have any direct or indirect liability or obligation, to pay any charges, claims or wages of any of the Bidder's employees, agents, contractors, and subcontractors.

The Bidder shall hold the Bank and it's RRBs, their successors, assignees and administrators fully indemnified and harmless against loss or liability, claims actions or proceedings, if any, that may arise from whatsoever nature caused to the Bank through the action of Bidder, its employees, agents, contractors, sub-contractors etc. However, the Bidder would be given an

opportunity to be heard by the Bank prior to making of a decision in respect of such loss or damage. The Bidder shall solely be responsible for all payments (including any statutory payments) to its employees and / or sub-contractors and shall ensure that at no time shall its employees, personnel or agents hold themselves out as employees or agents of the Bank, nor seek to be treated as employees of the Bank for any purpose, including claims of entitlement to fringe benefits provided by the Bank, or for any kind of income or benefits. The Bidder alone shall file all applicable tax returns for all of its personnel assigned hereunder in a manner consistent with its status as an independent contractor of services; and the Bidder will make all required payments and deposits of taxes in a timely manner.

3.2.42 AMENDMENTS

Other than the rights of the Bank specified in this Agreement, no change or modification of this Agreement shall be valid unless the same shall be in writing and signed by all the Parties.

3.2.43 COUNTERPARTS

This Agreement may be signed in any number of counterparts, each of which is an original and all of which, taken together, constitutes one and the same instrument.

3.2.44 GOVERNING LAW AND JURISDICTION

This Agreement 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 Agreement.

Survival of Clauses

Any provision or covenant of this RFP or subsequent Agreement, which expressly, or by its nature, imposes obligations beyond the expiration, or termination of this Agreement, shall survive such expiration or termination.

3.2.45 CHANGE CONTROL PROCESS

Any deviations or changes/amendment in the workflow of Services required by BANK may always be agreed between the parties, which shall be notified in writing BANK to BIDDER as change control process. Any other customization suggested by the Bank in the application or due to Regulatory requirement will be provided by Bidder without any additional charges to the Bank inter-alia provide any or all statutory/Regulatory report to the Bank free of Cost.

3.2.46 ACCEPTANCE OF TERMS & CONDITIONS

The Bidders participating in the tender process should give an Acceptance Certificate for all the points mentioned in the tender. Otherwise their offers are liable to be rejected.

3.2.47 NO LIABILITY OF THE BANK TOWARDS EMPLOYEES/ AGENTS OF SUCCESSFUL BIDDER

Notwithstanding anything contained hereinbefore and hereinafter, Bank shall not be liable in any manner for making any payment to any employee or agent of the successful Bidder (i) for the services rendered in and for Bank or for Bank by such employee or agent, as the case may be, towards performance of the contract to be entered into between Bank and the successful

Bidder, on express or implied instructions of the successful Bidder , and (ii) for any claim accrued or claimed to have accrued in favor of such employee or agent arising due to such services and /or due to any consequences of such services as aforesaid, under any law.

4. ELIGIBILITY CRITERIA

Eligibility criterion for the Bidders to qualify this stage is clearly mentioned in Annexure 4 – Eligibility Criteria Compliance to this document. The Bidders who meet ALL these criteria would only qualify for the second stage of evaluation. The Bidder would also need to provide supporting documents for eligibility proof. All the credentials of the Bidder necessarily need to be relevant to the Indian market. The decision of the Bank shall be final and binding on all the Bidders to this document. The Bank may accept or reject an offer without assigning any reason whatsoever.

4.1.1 ELIGIBILITY CRITERIA FOR BIDDER

The Bidder shall submit the proof to comply eligibility criteria as given below:-

Only those Bidders who fulfill the Pre-qualification criteria for Bidder and OEMs, as mentioned in Annexure 4 are eligible to submit response to this RFP.

Sr. No.	Eligibility Criteria	Supporting Documents
	Bidder's Financial & Other Information	
1	The Bidder should be a registered corporate in India, registered under the Companies Act 1956/ 2013.	Certificate of Incorporation
2	The bidder should have an average annual turnover of Rs.300 crore (Rupees Three Hundred Crores) per annum for last 3 financial years (i.e.	Copy of Audited Financial Statements (P&L and Balance Sheet) for the FY 2014-15, 2015-16 and 2016-17. In case of non-

Sr. No.	Eligibility Criteria	Supporting Documents
	2014-15, 2015-16 and 2016-17).	availability of audited financial statement for the 2016-17 bidder may submit the provisional statement certified by CA.
3	The bidder should be a profit making entity in each of the last three financial years viz. 2014-15, 2015-16 and 2016-17.	Copy of Audited Financial Statements (P&L and Balance Sheet) for the FY 2014-15, 2015-16 and 2016-17. In case of non-availability of audited financial statement for the 2016-17 bidder may submit the provisional statement certified by CA.
4	The Bidder and OEM should not be black-listed by any Public Sector Bank, RBI or IBA or any other Government agencies	Self-Declaration/ Undertaking to this effect to be submitted by the bidder
5	The bidder should have been operational in India for minimum of five (5) years as on 30/09/2017	Self-Declaration/ Undertaking to this effect to be submitted by the bidder
6	The Bidder must have presence in India and should have support center in Mumbai & Hyderabad.	Self-Declaration/ Undertaking to this effect to be submitted by the bidder
	Credentials and Experience	
7	The Bidder should have experience in implementing / supporting well-established Security Solutions for at least 2 BFSI clients in India out of which one should Scheduled Commercial Bank in India with at least 1000 branches.	Successful completion certificates or Credential Letters or Copy of Contract / Purchase order from the Client
8	The bidder should be providing IT security services / business (i.e. in the area of implementation, monitoring and management of various types of security solutions, devices, Technologies and software like (NAC/MDM/Brand Protection/ITSGRCM DRM/DDoS/Decoy/VM/HIPS/EE/ACC/API Management/FA/ATP/DLP) for a minimum period of three years as on the Date of RFP.	Successful completion certificates or Credential Letters or Copy of Contract / Purchase order from the client
9	The bidder must have minimum five (5) IT Security professionals having degree equivalent to Bachelor of Engineering (B.E.)/Bachelor of Technology	Self-Declaration/ Undertaking to this effect to be submitted by the bidder

Sr. No.	Eligibility Criteria	Supporting Documents
	(B.Tech) or more on their payroll with certification in CISA or CISSP or CISM or any other relevant / OEM professional certification in the field of IT Security.	AND Certification copies of the proposed resources
10	The Bidder must warrant that key project personnel to be deployed in this project have been sufficiently involved in the similar project in the past.	Self-Declaration/ Undertaking to this effect to be submitted by the bidder AND Bio-data of the personnel indicating their qualifications, professional experience and projects handled
11	Bidder should be either Original Equipment Manufacturer (OEM) of Security devices/software solutions or authorized partner of OEM. In case the bidder is an Authorized partner of the OEM, Bidder has to submit the authorization letter from the OEM.	Authorization letter on OEM's letterhead
12	Bidder is required to submit the OEM Associations and support agreement in the form Manufacturer's Authorization Form as annexed for this project letter on OEM letterhead.	Manufacturer's Authorization Form
13	OEM Experience (NAC, MDM, IT-SGRC, DRM, DDoS, HIPS, ATP, End point Encryption, Vulnerability Management, Brand Protection, Decoy, Application change control, API Management, Firewall Analyzer, Application Security testing, DLP): The proposed solutions must be available in India market for one or more years and successfully implemented in at least one BFSI organization in India with at least 1000 locations or regulatory bodies like RBI or payment autonomous bodies like NPCI.	Successful completion certificates or Credential Letters or Copy of Contract / Purchase order from the Bank

Note:-

- In the above matrix, "BFSI" refers to Banking, Financial services and Insurance organizations in India. (Excluding Regional Rural Banks and Scheduled Co-operative Banks)

- The Bidder shall not assign or sub-contract the assignment or any part thereof to any other person/firm without the consent of the Bank. In any case, the Bidder will be primarily responsible for all the activities under the scope.
- Bank reserves the right to change or relax the eligibility criteria to ensure inclusivity
- Bank reserves the right to verify / evaluate the claims made by the Bidder independently. Any deliberate misrepresentation will entail rejection of the offer
- The Bidder can be part of only one bid.
- In case an OEM submits a bid as a Bidder, then the OEM cannot participate through other Bidder's bids.
- In-case of corporate restructuring the earlier entity's incorporation certificate, financial statements, Credentials, etc. may be considered.
- 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.
- Bidders need to ensure compliance to all the eligibility criteria points.
- Purchase orders without relevant organization confirmation through a credential letter will not be considered as credentials.
- While submitting the bid, the Bidder is required to comply with inter alia the following CVC guidelines detailed in Circular No. 03/01/12 (No.12-02-6 CTE/SPI (I) 2 / 161730 dated 13.01.2012): 'Commission has decided that in all cases of procurement, the following guidelines may be followed:
 - ✓ In a RFP, either the Indian agent on behalf of the Principal/OEM or Principal/OEM itself can bid but both cannot bid simultaneously for the same item/product in the same RFP. The reference of 'item/product' in the CVC guidelines refer to 'the final solution that bidders will deliver to the customer.
 - ✓ If an agent submits bid on behalf of the Principal/OEM, the same agent shall not submit a bid on behalf of another Principal/OEM in the same RFP for the same item/product.'
- Proof of concept for the following solutions is mandatory prior to submission of the technical bid:
 - ✓ Application Change Control

Note: The Bidder can propose products from different OEMs for other in scope solutions. (Example: Bidder "A" can propose products from OEMs "B", "C" etc. for DRM, NAC etc.)

5. PROJECT TEAM STRUCTURE

All team resources included in implementation should be on the payroll of Bidder and/or OEM.

OEMs shall provide on-site resources at each deployment location for their respective solutions during the implementation phase in case the Bidder is not able to resolve the Bank's queries/ delays in implementation or as necessitated by Bank. It is mandatory for OEMs to do a post-implementation audit of respective solution wherever the Bidder proposes to perform implementation using its own resources.

For Implementation Team, Bidder will have teaming arrangement with respective OEMs and same shall be reflected in Bill of Material (BOM) as per Annexure 9. It shall be Bidder's responsibility to involve OEM/OEMs of respective solutions in each phased on implementation. The Bidder is not permitted to subcontract the ongoing operations (including facility management and project implementation team) of the solutions to other organizations.

5.1 PROJECT IMPLEMENTATION PHASE

During implementation phase, Bidder will place its team comprising of Bidders and OEM/OEMs resources for implementation of proposed solutions. The implementation team will be responsible for designing, implementation, integration, fine tuning and other activities required during implementation phase.

5.1.1 ROLES AND RESPONSIBILITIES

5.1.2 COMPREHENSIVE PROJECT MANAGEMENT SERVICES

The bidder is required to provide an experienced project manager for the tenure of the implementation, Go-live till successful completion of at least 2 DR drills. As part of the project management exercise the bidder is expected to

- Setup the project management office and framework comprising of:
 - ✓ Project charter formulation
 - ✓ Project risk analysis
 - ✓ Assistance in project management and project delivery team identification and resourcing
 - ✓ Change management procedures
 - ✓ Project planning and detailing
 - ✓ Project quality management procedures
 - ✓ Employ a formal project methodology on all projects undertaken with the level of detail and control scaled appropriately to the magnitude of the project effort and adhere to all project management processes and procedures
- Project Manage the following phases of the project :
 - ✓ Current State assessment
 - ✓ Business parameterization
 - ✓ Gap analysis and Customization
 - ✓ User Acceptance testing
 - ✓ Data migration, if any
 - ✓ Go-live/ Rollout
- Closure of issues pending for resolution

- Measure the progress made in the implementation of the project
- Track customization and gaps
- Monitor closure of gaps and customizations as per delivery schedules
- Provide regular updates to the steering committee and board as required by the Bank
- Participate in all technical and functional discussions relating to the projects
- The bidder is required to project manage the Go-Live and provide executive reports.

5.1.3 IMPLEMENTATION PROJECT MANAGER

A senior management member from the Bidder shall be identified as the project Manager (PM) who shall also be part of steering committee for implementation at Bank. The responsibilities of PM are outlined below:

- Lead implementation effort.
- Primarily accountable for successful implementation of the project across Bank.
- Act to remove critical project bottlenecks.
- Identification of working team members, and team leads.
- Single point of contact for Bank's senior management.
- Ensure implementation timelines are met to achieve desired result.
- Monitor Change management activities during implementation.
- Identify and implement best practices across Bank.
- Co-ordinate with OEM/OEMs for successful implementation of solutions.
- Periodic reporting to Bank on the implementation status, issues/ challenges faced and how these are handled.
- The project Manager shall be part of steering committee for implementation at Bank

5.1.4 TEAM LEAD FOR RESPECTIVE SOLUTIONS

A member from the Bidder implementation team shall be identified as the Team Lead (TL), whose responsibilities are outlined below:

- Lead daily implementation effort.
- Report on progress to PM and Bank.
- Identify and report any risks to PM and Bank.
- Seek advice from the PM on mitigation measures and deploy these at the Bank handled by the team lead

5.1.5 IMPLEMENTATION TEAM

The implementation team's responsibilities are outlined below:

- Implementation of all devices in scope across Bank.
- Customize devices as per requirements.
- Perform acceptance testing for each device/solution.

5.1.6 OEM TEAM

OEMs shall also provide on-site resources at each deployment location for their respective solutions during the implementation phase. The OEM officials will be responsible for:

- Validation of solution design and architecture
- Continuous monitoring of implementation at each location
- Provide Subject Matter Expertise support to working teams.
- Ensure customization is in line with Bank's requirements.
- OEM sign off would be necessary after implementation of its products
- Perform post-implementation audit of solutions where the Bidder proposes to implement a solution without involving OEMs resources.
- In addition to this, OEM/OEMs will also perform half-yearly/Yearly health check-up of their solutions implemented in Bank and provide comprehensive report to Bank.

5.2 OPERATION PHASE

Bidder and OEM has to sign off the proper implementation and documentation and provide handover to Bank personnel and SOC team for further monitoring and seamless operation.

6. BIDDER EVALUATION & METHODOLOGY

The evaluation will be conducted in the following stages:

1. Technical Bid Evaluation
2. Commercial Bid evaluation

The objective of evolving this evaluation methodology is to facilitate the selection of the most optimal solution that appropriately meets the business requirements of the Bank. The bidders would be screened based on General Eligibility Criteria. Post qualification of a Bidder on these criteria, bid would be evaluated on technical soundness. All bids shall be evaluated by an Evaluation Committee set up for this purpose by the Bank. The evaluation shall be on the basis of quality of the solution & services offered and cost of the offered solution and services. Bidder's qualifying the technical bid evaluation will be considered for commercial evaluation.

The decision of the Bank would be final and binding on all the Bidders to this document. The Bank may accept or reject an offer without assigning any reason what so ever.

6.1 NORMALIZATION OF BIDS

The Bank will go through a process of technical and commercial evaluation and normalization of the bids to the extent possible and feasible to ensure that Bidders are more or less on the same technical ground. After the normalization process, if the Bank feels that any of the bids need to be normalized and that such normalization has a bearing on the commercial bid; the Bank may at its discretion ask all the technically shortlisted Bidders to resubmit the updated technical and commercial bids once again for scrutiny. The Bank can repeat this normalization process at every stage of technical submission till the Bank is reasonably satisfied. The Bidders agree that they have no reservation or objection to the normalization process and all the technically short listed bidders will, by responding to this RFP, agree to participate in the normalization process and extend their co-operation to the Bank during this process. The Bidders, by submitting the response to this RFP, agree to the process and conditions of the normalization process. Any non-compliance to the normalization process may result in disqualification of the concerned Bidder.

Bank may call for any clarifications/ additional particulars required, if any, on the technical/ commercial bids submitted. The Bidder has to submit the clarifications/ additional particulars in writing within the specified date and time. The Bidder's offer may be disqualified, if the clarifications/ additional particulars sought are not submitted within the specified date and time. Bank reserves the right to 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. Central Bank of India also reserves the right to conduct reference site visits at the Bidder's client sites. Based upon the final technical scoring, short listing would be made of the eligible bidders for final commercial bidding.

6.2 GENERAL ELIGIBILITY CRITERIA

Central Bank of India shall scrutinize the Eligibility bid submitted by the Bidder. A thorough examination of supporting documents to meet each eligibility criteria (Annexure 4) shall be

conducted to determine the Eligible bidders. Bidders not complying with the eligibility criteria are liable to be rejected and shall not be considered for Technical Evaluation.

The Bidder meeting the General Eligibility Criteria as per Annexure 4 will be considered for technical evaluation. Any credential/supporting detail mentioned in “Annexure 4” and not accompanied by 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.

PROCESS

6.3 TECHNICAL EVALUATION

The objective of this evaluation process is to facilitate the selection of the most optimal solutions that appropriately meets all requirements of the Bank. All bids shall be evaluated by an evaluation committee setup for this purpose by the Bank. The Bank will evaluate the technical offers of the Bidders in terms of eligibility criteria and the proposals meeting the criteria will only be taken up for further technical evaluation. The decision on the Bank in regards to evaluation would be final and binding on all the Bidders to this document. The Bank may accept or reject an offer without assigning any reason whatsoever.

The technical evaluation criterion would broadly involve the following major areas:

- **Compliance to the bill of materials as in Appendix 1 (masked)**
 - ✓ The Bidder is expected to provide their ‘compliance’ against each item stated in the Bill of material, this means that the Bidder confirms to the provisioning of the stated product / service and the terms of the RFP and subsequent addendums. Deviations to the Compliance requirements may lead to disqualification.
- **Compliance to the technical specification as in Annexure 7** - The Bidder is expected to provide their ‘compliance’ against each item stated in the Annexure 7, this means that the Bidder confirms that the proposed solution meets the technical specification mentioned in Annexure 7.
- **The design documentation**
- **Bidder’s detailed work plan** – Bidder to share gnat chart in conformity with the stated timelines. The Bidder should also share the key profiles and the number of representatives (across OEMs as well) being deployed across the Implementation Phase and the Support phase of the project.
- **Technical Presentation** - As part of technical bid, Bidder will also submit their approach methodology covering each of the activities and the proposed implementation schedule. The Bidders shall be invited to the Bank to deliver a presentation for about 60 minutes on the solutions that are proposed. The presentations would be rated by a competent panel chosen appropriately by the Bank and scores would be assigned to each of the presentations. The Bidders are expected to submit the soft copy of the presentation to the Bank prior to the presentation.
- **Site Visit** - Bank at its discretion may visit any or all reference sites where Bidder has implemented the solutions.

The technical soundness will be rated as follows:

Sr. No.	Technical Criteria	Maximum Score	Minimum Score	Minimum %
1	100% Compliance to the Scope of Work	100	100	100%
2	100% Compliance to the technical specification as in Annexure 7 - Minimum technical specification	100	100	100%
3	Bidder's Technical Presentation	50	37.5	75%
	Maximum Score – Technical Evaluation	250	237.5	

The Bidder must satisfy BOTH of the following two categories to qualify for commercial evaluation (Stage 3).

- *The Bidder must comply to scope of the requirement as set out in the RFP and*
- *The Bidder must comply to all the line items in Appendix 1- Bill of Materials indicated by The Bank as ““(Bidder shall provide their compliance here)” in column “Bidder compliance (Yes/No)” AND*
- *The Bidder must achieve minimum score of 75% of Bidder's Technical Presentation to qualify for the Commercial evaluation*
- *Marks provided by the Bank to the Bidder shall be final. No objection/query/justification related to given marks from any Bidder shall be entertained. Decision of Bank in this regard shall be final & binding*
- *It is to be noted that Bank will only disclose final marks to technically qualified Bidders*

Bidders are required to comply with the requirements stated herein, if any Bidder's response is found to be non-compliant, then The Bank at its discretion may reject the Bid. Hence only the Bidders who have achieved the set compliance will be considered for commercial bid evaluation.

At the sole discretion and determination of the Bank, the Bank may add any other relevant criteria for evaluating the proposals received in response to this RFP.

Bank may, at its sole discretion, decide to seek more information from the respondents in order to normalize the bids. However, respondents will be notified separately, if such normalization exercise as part of the technical evaluation is resorted to.

The commercial proposals of technically short listed Bidders will then be opened.

6.4 COMMERCIAL EVALUATION

The commercial bid of only those bidders shall be opened who have been technically qualified on the basis of the technical proposal. These technically qualified bidders as per technical evaluation process will participate in Reverse Auction process, if conducted by the Bank. The

bank will notify the date and time for participating in the online reverse auction process to the technically qualified bidders.

The envelope containing 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 Annexure 9. The commercial offer should consist of comprehensive Cost for required solution. Bidder must provide detailed cost breakdown, for each and every categories mentioned in the commercial bid. The Bank will determine whether the Commercial Bids are complete, unqualified and unconditional. The technically qualified bidders may be required to participate in the reverse auction. 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.

6.4.1 REVERSE AUCTION

Bank would conduct a reverse auction process on the commercials submitted by the Bidders. As such it is necessary that authorized personnel of the firm or organization sign the Bid. The designated personnel should be authorized by the organization or by a senior official of the organization having authority to do so. The same person or a different person should be authorized, who should have digital certificate issued in his name and should have authority to quote bid amount in the commercial bid and also quote offer price during on-line reverse auction. The details of digital certificate like Name, Digital Key details, issuing authority and validity etc. to be provided.

The certified xerox copy of necessary Original resolutions/authority/ Power of Attorney having authority to authorize the person to submit Bid documents/participate in on-line sealed bid and reverse auction, on behalf of the company shall be enclosed. The proposal must be accompanied with an undertaking letter duly signed by the designated personnel providing a Bid commitment.

Bidders to note that:

- In case there is variation between numbers and words; the value mentioned in words would be considered.
- The Bidder needs to provide unit costs for all components and services; unit rates would be considered for the TCO in case of any discrepancy in the totaling, modifications, addition, correction, etc.
- In the event the Bidder has not quoted or has omitted any mandatory product or service required for the Solution it shall be deemed that the Bidder shall provide the product or service at no additional cost to the Bank.

Please note that in the event of the Bank conducting a normalization exercise, the bids submitted after normalization would be evaluated as per the evaluation methodology in Commercial Evaluation. Bidder categorized as L1 after the Normalization process would be deemed as the Successful Bidder.

6.4.2 COMMERCIAL BID EVALUATION CONSIDERATIONS

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

- If there is a discrepancy between words and figures, the amount in words shall prevail
- If there is a discrepancy between percentage and amount, the amount calculated as per the stipulated percentage basis shall prevail
- Where there is a discrepancy between the unit rate and the line item total resulting from multiplying the unit rate by the quantity, the unit rate will govern unless, in the opinion of bank, there is an obvious error such as a misplacement of a decimal point, in which case the line item total will prevail
- Where there is a discrepancy between the amount mentioned in the bid and the line item total present in the schedule of prices, the amount obtained on totaling the line items in the Bill of Materials will prevail
- The amount stated in the correction form, adjusted in accordance with the above procedure, shall be considered as binding, unless it causes the overall price to rise, in which case the bid price shall prevail
- If there is a discrepancy in the total, the correct total shall be arrived at by bank
- In case the bidder does not accept the correction of the errors as stated above, the bid shall be rejected.
- At the sole discretion and determination of the bank, the bank may add any other relevant criteria for evaluating the proposals received in response to this RFP.
- Bank may, at its sole discretion, decide to seek more information from the respondents in order to normalize the bids. However, respondents will be notified separately, if such normalization exercise as part of the technical evaluation is resorted to.
- All liability related to non-compliance of this minimum wages requirement and any other law will be responsibility of the bidder.
- The bank shall not incur any liability to the affected bidder on account of such rejection.
- The selected bidder shall provide revised TCO and the revised break-up of the cost items post reverse auction.

The commercials will be calculated till two decimal points only. If the third decimal point is greater than .005 the same shall be scaled up else it shall be scaled down to arrive at two decimal points. Bank will make similar treatment for 4th or subsequent decimal point to finally arrive at two decimal points only.

7. 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 80%, 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.

7.1 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:

7.2 PRODUCT COST

Sl. No.	Deliverables	% of Payment	STAGES (On completion of the activities)
1	Hardware Appliance /	60%	60% cost would be payable on successful post-delivery inspection of the product
		30%	30% cost would be payable on successful installation and acceptance testing of the product
		10%	10% cost would be payable after installation which shall be released earlier against a Bank guarantee of an equivalent amount

2	Software / License	80%	80% cost would be payable on successful post-delivery inspection of the product
		20%	20% cost would be payable on successful installation and acceptance testing of the product
3	Installation & Commissioning	80%	80% cost would be payable on successful installation and acceptance testing of the product
		20%	20% cost would be payable after 1 month of successful installation of the solutions
4	Payment for deployment of endpoint solutions (DRM, Endpoint encryption, NAC)	90%	90% cost would be payable on successful deployment of 80% users, nodes or devices across the network for the respective solution
		10%	10% cost would be payable on successful deployment of 20% users, nodes or devices across the network for the respective solution
5	FM Support (if applicable)		Payment for on-site support charges will be paid quarterly in arrears.
6	Training	100%	100% cost would be payable post successful completion of the training to the designated officials

General Conditions:

- There shall be no escalation in the prices once the prices are fixed and agreed by the Bank and the Bidder
- All applicable taxes and duties will be deducted at source as per applicable laws
- Any penalties / liquidated damages imposed on the Bidder for non-performance will be deducted from the payment as deemed necessary

Delivery, implementation and Roll out:

The Selected Bidder shall be responsible for delivery; implementation and rollout of all the solutions required under this RFP and also must agree to the timeline as specified above.

In the event of Bidder's failure to deliver and/or implement all required components of a fully functional system (pertaining to the scope of the project) within the stipulated time schedule or by the date extended by the Bank, unless such failure is due to reasons entirely attributable to the Bank, it will be a breach of contract. In such case, the Bank would be entitled to charge a penalty or will have the right to terminate the contract, as specified in this RFP.

7.3 AMC & ATS AND OTHER WARRANTY COSTS

The Bidder shall provide the maintenance (Warranty, AMC & ATS) for a period of five years beginning from the date of solution acceptance test sign-off. The Warranty period for the 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. The Bidder must factor the costs in the Bill of Material accordingly. As part of warranty, AMC & ATS support the Bidder has to:

- Bidder is required to provide the services for a period of 5 years.
- Post completion of the contract / or in the event of early termination, the Bidder is expected to provide support for transition of the services to the nominated members of the Bank (or) to a third party nominated by the Bank.
- Provide on-site comprehensive support for security equipment and software components provided as part of this RFP
- Back to back agreement with respective OEMs for the maintenance services (Warranty/AMC/ ATS)
- Warrant all the security equipment and software 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 security equipment and software
- Provide for maintenance of security equipment, including preventive maintenance support, as well as repair or replacement activity after a 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. 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 the support services like repair, replacement to resolve the problem as per the service levels defined in Section 2.4.
- Defective security equipment shall be replaced by the Bidder at his own cost, including the cost of transport etc. The Bidder shall not charge the Bank for any extra charges related to this activity, during the period of contract
- Provide on-site support during quarterly DR drills or whenever required by the Bank. For factoring purposes, the Bidders should factor not more than 8 visits at DC or DR each year for on-site support on specific request from the Bank
- Agree that 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 the Bidder during the period of warranty
- Undertake system maintenance and replacement or repair of defective security equipment
- Upon receipt of such notice the Bidder shall, as mentioned below, repair or replace the defective goods or parts thereof, without any cost to the Bank
- In case equipment taken away for repairs, the 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, the 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, then the OEM shall transfer such services to that preferred Bidder at no additional cost to the Bank
- In case of any issue with security equipment and related software supplied by the Bidder, Bank or its appointed System Integrator shall log a call with the Bidder (who has supplied the security equipment/software); it is responsibility of the Bidder to resolve the issue with the assistance of the OEM is deemed necessary. The Bank or its appointed System Integrator shall promptly notify the Bidder in writing / e-mail / fax 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 warranty free of cost
- The Bidder warrants that the equipment 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
- The Bidder further warrants that all the equipment 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 the Bidder, that may develop under normal use of the supplied Goods in the conditions prevailing at the final destination
- The Bidder's hardware engineer will report at the Bank's premises within one hour of reporting of breakdown through telephone/ email or Fax or courier at the Bidder's nearest office and repair the same at the earliest

The Bidders are expected to provide technical and commercial proposals in accordance with the terms and conditions contained herein. Evaluation criteria, evaluation of the responses to the RFP and subsequent selection of the successful Bidder shall be as per the process defined in this RFP. Their decision shall be final and no correspondence about the decision shall be entertained.

Security Solutions:

The Bidder needs to ensure that the bid must include a minimum comprehensive on-site free warranty of 3 years from the date of installation and acceptance testing sign off of the system by the Bank including all parts and labor. No parts, accessories of the systems should be excluded from such warranty.

Also the offer includes AMC of 2 years from expiry of the warranty period. During the AMC period, the services rendered by the Bidder should be the same as those extended during the Warranty period.

Software updates/Upgrades:

All software updates/upgrades during the period of contract Five (5) years have to be provided at no cost to the Bank. All technical support issues related to software like bugs, problems with the product software causing the service disruptions have to be attended as per the SLA terms mentioned in this RFP. It is responsibility of the Bidder/ OEM that the software solution shall function at satisfactory level during the period of the contract.

All software supplied will carry following warranty:

- Media warrantee for 90 days.
 - Patches and software/product updates and upgrades for 5 years.
-
- ✓ Bidder shall be fully responsible for the manufacturer's warranty in respect of proper design, quality and workmanship of all equipment, accessories etc. covered by the tender.
 - ✓ Bidder must warrant all equipment, accessories, spare parts etc. against any manufacturing defects during the warranty period.
 - ✓ During the warranty period of contract Bidder shall maintain the systems and repair/replace at the installed site, at no charge to the Bank, all defective components that are brought to the Bidder's notice.
 - ✓ The Bidder shall carry out Preventive Maintenance (PM), including cleaning of interior and exterior, of all hardware and testing for performance once in a calendar quarter and should maintain proper records of the same.
 - ✓ As far as possible, the equipment should be repaired at site and where the equipment is taken for repairs outside the Bank, a substitute of the similar or higher configuration / capacity equipment should be provided and data should be transferred to the substitute machine besides creating back-up.

8. DEFINITIONS & REFERENCE

8.1 WORKING DAY

A working day would be any day any branch / office of the Bank is functioning.

8.2 BUSINESS HOURS

Business Hours for the purpose of service standards would be 8.00 am to 8.00 pm., on all working days. However, the complete hardware infrastructure in the DC, NS & DR would need to function 24*7 to service the Bank's business.

8.3 RESTORE TO SERVICE

Provides standard maintenance services including:

- Diagnostics and troubleshooting
- System, component & hardware maintenance
- Configuration changes, tracking, and documentation
- Upgrade / Enhancement

The maintenance for the services would be for the entire business infrastructure of the Bank including, but not limited to software, servers and all network and security equipment supplied under this scope.

8.3.1 OBLIGATION OF THE BIDDER

In the course of rendering the services mentioned in this RFP, Bidder shall be responsible for the following:

- Bidder shall assign personnel of appropriate qualifications and experience to perform the services in order to fulfill its obligations.
- Bidder shall designate one of its personnel as the Project Manager, to interact with the Designated Customer Support Contact from the Bank for the purposes of getting approvals, progress report, discussing and resolving issues, arranging meetings, etc.
- Bidder shall exercise requisite control and supervision over its personnel in the course of rendering the services and make best efforts to ensure that the services are rendered in a continuous and uninterrupted manner.
- Bidder will have the right to withdraw its personnel, by replacing the persons with others having appropriate experience and skills at its own cost. Bidder shall seek necessary permission from the Bank 1 month in advance.
- In the event that any person engaged/deputed/deployed for rendering services, is, either; No longer available by reason of resignation or termination or the like; or unable to render satisfactory services; or not acceptable to the Bank by reason of any misconduct or non-performance on the part of such person.
- Bidder will use all reasonable endeavors to replace such individual promptly by another sufficiently skilled, qualified, and experienced with appropriate certifications personnel at its own cost. Bidder will in the discharge of its obligations use all reasonable endeavors to minimize changes in personnel.
- Bidder will respect the confidentiality of all information given to it by the Bank and will not divulge such information to any third party or other units without the consent of the Bank.

8.4 OBLIGATION OF THE BANK

The Bank shall be responsible for the following:

- The Bank shall designate a Customer Support Contact for each designated location who shall be a single point of contact between the Bank and Bidder for all communication in connection with the provision of delivery services. The Parties also agree that all interaction and communication between the Parties for the purposes of this tender shall take place through the Customer Support Contact designated by the Bank. Bidder shall not be required to incorporate any direct input received from the Named Users, unless expressly ratified by the Customer Support Contact of the Bank in writing.
- The Bank shall ensure that all requests for support services are formally raised in accordance with the procedure prescribed in respect thereof and all such requests conform to the formats agreed upon from time to time.
- The Bank shall give Bidder and its personnel full access (physical and/or remote) to the Support Location, and the designated hardware & Equipment to enable Bidder to provide the Maintenance & Support Services.

9. DISCLAIMER

The RFP document is not an offer made by Central Bank of India but an invitation for response based on which the Bank may further evaluate the response or call for alternate or more responses from other Bidders. The Bank has the right to ask for other competitive quotations and can award any part or complete work to another Bidders whom so ever they feel eligible for the same taking into consideration the price and quality.

End of Document