

Request for Proposal for Supply,
Implementation and Maintenance of IT
Security Solutions



REQUEST FOR PROPOSAL (RFP)

For

Supply, Implementation and Maintenance of IT Security Solutions

(Disk/folder/file/ USB encryption, Data Classification,
Application Whitelisting, File Rights Management (FRM),
Mobile Device Management (MDM) and Secure Web Proxy)

Ref: BOI:HO:IT:SS:0070

Dated: 02.05.2020

BANK OF INDIA, HEAD OFFICE

INFORMATION TECHNOLOGY DEPARTMENT

Bank of India, a body corporate, established under the Banking companies (Acquisition and Transfer of Undertakings) Act 1970, having its Head Office at Bank of India, Star House, 'G' Block, Bandra Kurla Complex, Bandra (East), Mumbai – 400 051, India intends to do **procurement, commissioning, installation, implementation, maintenance, monitoring and management of IT Security Solutions for its domestic, and foreign branches/offices**, invites bids from the eligible bidders, to participate with complete installation, commissioning, integration and maintenance of **IT Security Solutions** at all branches/offices which includes all domestic, RRBs and foreign branches/offices as per the specifications, terms, conditions and scope given in detail in this RFP, for a period of 5 years .

The Bidding Documents include:

- (a) PART 1 - Invitation to Bid (ITB)**
- (b) PART 2 - Disclaimer**
- (c) PART 3 - Instruction for Bidders (IFB)**
- (d) PART 4 - Terms and Conditions of Contract (TCC)**
- (e) PART 5 - Functional Specifications (FS)**
- (f) PART 6 - Bid Forms, Price Schedules and other formats (BF)**
- (g) PART 7 - Other Terms and Conditions. (OTC)**

PART 1: INVITATION TO BID (ITB)

Introduction

The Bank has an operational IT Operations Centre and Cyber Security Operations Centre (C-SOC). However, in view of the growing use of IT, the evolving new threat environment and RBI requirements, Bank has decided to purchase additional security solutions to enhance the security posture of the Bank.

Bank intends to invite offers from interested System Integrators (SIs)/ OEMs to bid for, Supply, Installation, Integration, Implementation, Operations and Maintenance of Security Solutions, and integrate with Bank's existing setup (applications and hardware). The selected Bidder will be responsible for implementing security solutions at the Bank's DC and DR site and Roll-out till branch locations. Selected Bidder will also supply and install all required infrastructure as per the broad objectives as outlined in this RFP and for this purpose Bank invites quotes for the same as per the specifications as indicated in Part 5 Functional Specification. The prices quoted in the Price Bid shall remain valid for the entire contract period, however for any additional procurement / repeat order within contract period, Bank may refer to the bidder's quoted price.

Under FMS, bank may procure additional manpower at same rates (as quoted), during the contract period.

You are requested to send your Technical and Price proposal as per the enclosed formats. The methodology for submission of the proposals is enumerated in Part 3 Instruction to Bidders. Terms and Conditions of Contract (TCC) are given in Part 4. The various forms, formats and Performa are given in Part-6 which mandatorily to be submitted by the bidder along with bid.

The Bidding Document may be obtained from the Bank as under or downloaded from Bank's Website <http://www.bankofindia.co.in/tenders> and the bid should be submitted to the office of Bank Of India , Information Technology Department, Head office, Star House-2, C-4, G-Block, 8th Floor, West Wing, Bandra Kurla Complex, Bandra (East) Mumbai – 400051(Telephone No. 022-61319866/ 61319840). E-Mail: Head Office - IT (HeadOffice.IT@bankofindia.co.in)

- ❖ For queries and clarification regarding the RFP, please feel free to contact us at the above mentioned address or telephone number or e-mail id. During pre-bid meeting, all queries submitted by interested eligible bidders shall be discussed. After pre-bid meeting, the queries cannot be considered.
- ❖ Please note that all the information desired about the tender need to be provided to us. Incomplete information may lead to rejection of the bid/non-selection.
- ❖ All Bids must be accompanied by Bid Security as specified in the Bid document.

- ❖ Tender Fee - A non-refundable bid amount of Rs.50,000/- to be paid by means of a demand draft / pay order/pay slip favoring “**Bank of India**” payable at Mumbai from **any Scheduled commercial /Nationalized Bank other than Bank of India.** . If the bid is downloaded from website, the cost of the bid/tender fee may be paid along with the technical bid in a separate envelope.
- ❖ The earnest money deposit (EMD) for the bid is of Rs. 50,00,000/- (Rs. Fifty Lakhs Only) by way of Bank Guarantee (format as per **FORMAT 6.6**) from any of the Scheduled commercial / Nationalized banks of India (other than Bank of India) in an acceptable form favoring “**Bank of India**” – EMD for Procurement, Installation, Commissioning, Maintenance, Monitoring and Facility Management of IT Security Solutions for Domestic, Foreign Branches/ subsidiaries/ Offices RFP Ref: BOI:HO:IT:SS:0070 dated: 02.05.2020, at Mumbai. No interest shall be allowed on the Earnest Money. Bids without Earnest Money are liable for rejection.
- ❖ Bank reserves the right to change the dates mentioned below or in the RFP, which would be communicated by way of corrigendum published on Bank’s Corporate Website.
- ❖ In this regard, a two-envelope bidding Procedure (Technical Bid and Price Bid) in separate envelopes will be adopted. The technically complete and commercially competitive bids shall be submitted in two parts viz. **qualifying and Technical Bid – Part A and Price Bid – Part B in separate sealed cover.**
- ❖ The Bids should be delivered to the address mentioned below with acknowledgement due so as to reach before **15.00 hours** on or before **29/05/2020**. If the last day of submission of bid is declared holiday under **Negotiable Instruments Act** by the Government subsequent to the issuance of RFP, the next working day will be deemed to be the last date of submission of the Bid. The bids, which are received after the above mentioned date and time, are liable to be rejected at the discretion of the Bank.
- ❖ The Bank shall not be liable for non-delivery of documents due to Postal/Courier delay or loss of documents in transit etc., if any, in submitting the Bid. The Qualifying & Technical Bid shall be opened in the presence of Bidders on **29/05/2020** at **16:00 hrs.** in the below mentioned Premises. The Bidder’s representative may be present during the Technical Bid opening at our Office well in time along with the authorization letter from the bidder’s company.

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**

बैंक ऑफ़ इंडिया
Bank of India **BOI**



❖ The important dates / schedules for the above RFP shall be as following:

Date and time of commencement of inspection / Sale of Bid Document	02/05/2020
Last date and time for Pre Bid Queries	11/05/2020 till 15:00 Hrs.
Pre Bid meeting date, time and venue	13/05/2020 15:00 Hrs. Venue: Bank of India Star House-2, 'G' Block, Head Office, I.T. Department; 8 th floor, Bandra Kurla Complex, Bandra (East), Mumbai – 400 051
Last date and time for Receipt of Bids at Bank of India (address as given below)	29/05/2020 15.00 hrs.
Date and time of opening of Technical Bids	29/05/2020 16.00 hrs.
Address for communication and Submission of bid.	The General Manager, IT Department Bank of India Star House-2, 'G' Block, Head Office, I.T. Department; 8 th floor, Bandra Kurla Complex, Bandra (East), Mumbai – 400 051
Bid document availability	Bidding document to be downloaded from the Tender section of our Bank's web-site www.bankofindia.com

❖ For any technical clarification, the contact person are Shri Ajay Kapoor, Chief Manager email- Ajay.kapoor@bankofindia.co.in, Ph. No. 022-61319890 and / or Shri Mayank Tandon, Senior Manager email- Mayank.Tandon@bankofindia.co.in Ph. No. 022-61319866.

PART 2: DISCLAIMER

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

This RFP is neither an agreement nor an offer and is only an invitation by Bank to the interested parties for submission of bids. The purpose of this RFP is to provide the bidder(s) with information to assist the formulation of their proposals. This RFP does not claim to contain all the information each bidder may require. Each bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP and where necessary obtain independent advice. Bank makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. Bank may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

3. INSTRUCTIONS FOR BIDDERS (IFB)
TABLE OF CLAUSES

Clause No.	Topic	Clause No.	Topic
	A. Introduction		D. Submission of Bids
3.1	Introduction	3.19	Sealing and Marking of Bids
3.2	Broad Scope of Work	3.20	Deadline for Submission of Bids
3.3	Detailed Scope of Work	3.21	Late Bids
3.4	Eligibility Criteria	3.22	Modification & Withdrawal of Bids
3.5	Cost of Bidding.		E. Bid Opening and Evaluation
	B. Bidding Documents	3.23	Opening of Bids by the Bank
3.6	Content of Bidding Documents	3.24	Clarification of Bids
3.7	Clarification of Bidding Documents	3.25	Preliminary Examination
3.8	Amendment of Bidding Documents	3.26	Technical Evaluation
	C. Preparation of Bid	3.27	Opening of Price Bids
3.9	Language of Bid	3.28	Contacting the Bank
3.10	Format and signing of the Bid		F. Award of Contract
3.11	Documents comprising the Bid	3.29	Post-qualification
3.12	Bid Submission	3.30	Bank's Right to Accept Any Bid and to Reject Any or All Bids
3.13	Bid Prices	3.31	Award Criteria
3.14	Bid Currencies	3.32	Notification of Award
3.15	Documents establishing Bidder's Eligibility and Qualifications	3.33	Signing of Contract
3.16	Documents establishing eligibility of products & conformity to Bid Documents	3.34	Performance Security
3.17	Bid Security	3.35	Contract Start date and Duration
3.18	Period of Validity of Bids		

3. INSTRUCTIONS FOR BIDDERS (IFB)

A. Introduction

3.1 Introduction

Bank of India (hereinafter referred as Bank), having registered office in Mumbai, is one of the largest public banks in India with a Branch network of more than 5000 branches in India and 49 branches/offices in 21 countries overseas.

Bank has setup its Data Center (DC) at CBD Belapur, Mumbai, Disaster Recovery (DR) Site at Bengaluru, and Near Site (NR) at CBS Belapur, Mumbai.

Bank is also have its sponsored Regional Rural Banks (RRBs) i.e. Narmada Jhabua Gramin Bank (NJGB), Aryavart Bank (AB) and Madhya Pradesh Gramin Bank (MPGB) with a total branch network of more than 2500 Branches.

3.2 Broad Scope of Work

- 1) Bank intends to procure security solutions to enhance the security posture of the Bank. For this, Bank invites proposals from well experienced bidders for supply, implementation, rollout, operations of the 6 Security solutions and integration with the C-SOC (Cyber Security Operations Centre) Solutions and other existing solutions/ related infrastructure in Bank. If any Professional services efforts are required from OEMs of new solutions, the costs should be included in RFP quotes. The bidder shall coordinate with on-site management Teams for integration of newly procured security solutions with existing solutions. The Term of contract shall be of 5 years.
- 2) All the Solutions should be deployed in the Bank's DC/DR Setup. The public Cloud based solutions should not be proposed under this RFP and if proposed, will not be considered.
- 3) The solutions should be designed in such a way that they cover all the divisions of the Bank's Data Center i.e. Domestic, Foreign and its RRB /associates/subsidiaries/ having separate networks & all separate network segments of each. Presently procurement is for domestic and FCBS Branches. However, Bank at its discretion, may use and/or procure (any /all) solution and its licenses as per the same quoted rates for RRB /associates/subsidiaries upon arising the requirements for RRBs. Moreover, Bank reserves the right to use/

relocate the licenses procured for Domestic/ FCBS interchangeably to RRB /associates/subsidiaries. The proposed solution should be configured and scalable to cater the requirement of implementation of these solutions for the solution deployment should be compliant with Bank's IS, IT and Cyber policies, internal guidelines, regulatory requirements and country wide regulations and laws from time to time.

- 4) At a minimum, the new solutions should effectively and efficiently manage operations and security posture of the Bank by preparing for and responding to cyber risks/threats, facilitate business continuity and recovery from cyber attacks / incidents.
- 5) The solutions should be able to integrate various log types and logging options into SIEM, with Active Directory for user authentication, with HP Service Manager or any other standard ticketing tool for ticketing/workflow/case management, unstructured data/big data, reporting/dashboard, use cases/rule design (customized based on risk and compliance requirements/drivers, etc.), with IT-GRC Solution etc. The Proposed Security solutions should be in adherence to the guidelines provided in the RBI cyber security circular no RBI/2015-16/418 dated 2nd June 2016 and its amendments (in present and in future).
- 6) The solution should have capability to integrate with IT Service management tools. At present, the Existing Ticketing solution of HP SM is used as IT Service Management Tool. For event managements/logs, SIEM Solution from IBM (Q-Radar) is deployed in Bank's environment.
- 7) In line to Scope, the OEM certified deployment methodology shall be followed and submitted by the bidder as part of Implementation Plan duly signed by OEM and Bidder.

3.3 Detail Scope of Work

3.3.1 The Bank has decided to procure and implement the following solutions:

1. Disk/folder/file/ USB encryption Solution
2. Data Classification Solution
3. Mobile Device Management Solution
4. Application Whitelisting
5. File Right Management Solution
6. Secure web gateway/web proxy solution

General Requirements for purchase of security solutions

- 1) Bank is not liable or bound to procure all the 6(Six) solutions mentioned in the earlier section at once. Bank may undertake phase wise procurement, supply, installation, and implementations of the solution(s) and its licenses.
- 2) Bank may procure products with required quantity (not limited to specific number) and may remove any solution at any stage, at its sole discretion, till issuance of PO from proposed solutions list that are part of this RFP.
- 3) Considering the nature of the tools, it may happen that the bidder may propose a solution suite consisting of multiple features, functionalities suiting to the RFP requirements and in compliance of RBI cyber security circular no RBI/2015-16/418 dated 2nd June 2016 and its amendments (in present and in future). The bidder shall provide the solutions with all such features (over and above to technical specifications) without any extra cost to the Bank. All the available functionalities should be available to the Bank. The bidders are requested to make necessary provisions and include complete cost in the respective line items of price schedule of the solution.
- 4) The cost of each of the line items (for each of the solution) as mentioned in the RFP has to be mentioned at appropriate place in the respective formats. The separate addendum can be submitted for clarifications of line items (if required) as per BOM and which be a part of a solution suite by the bidder and forms an integral part of the solution. Bank shall not make any payment other than line items mentioned in the price bid format.
- 5) The Bank has its captive Security Operations Centre (SOC) in place and is functional round the clock. The proposed solutions should be able to seamlessly integrate with SOC/existing solutions including Network Operation Center (NOC) and any future solutions procured by the bank, during the contract period and in future. The Integration work will be responsibility of bidder failing which Bank may reject the procurement without payment of any cost or liability(including license cost) to the Bank.
- 6) If a solution fails to meet the technical requirements of RFP during the implementation/ before sign-off phase, Bank reserves the right to reject the solution with no cost to the Bank and recover all liquidated damages from the amount payable for other solutions procured. Even after, the Bank is unable to recover the amount, the bank at its discretion can invoke Performance Bank Guarantee as submitted. However, in such cases the bidder may offer alternate solution to the Bank which fulfils technical specifications/ requirements of the RFP with no extra cost to the Bank. Liquidated damages/penalty shall be applicable for delay beyond the stipulated timelines.

- 7) The Bidder would be responsible for supply, installation, testing, commissioning, configuring, Operation & Maintenance of the solutions, warranty and AMC of licenses (hardware, software, middleware supplied) as part of this RFP for a period of 5 years.
- 8) During the period of the contract, all upgrades/updates or requirements in hardware, software, licensing, implementation of upgrades/patches/version changes etc., due to whatsoever reason including but not limited to EOL or EOS, shall be done by the bidder without any additional cost to the bank. EOS/EOL solution will not be accepted and if any solution is declared EOS/EOL during period of contract, bidder shall upgrade the same well before its EOS/EOL without any additional cost to the bank. Non-availability of services of solutions shall be counted as downtime.
- 9) For Sign-off of the successful commissioning of the solution, post installation and commissioning of appliance & software at all locations (DC and DR), all respective technical/statutory parameters, validations and SCD should be implemented, checked & verified and related reports including SOP, SCD, Software Integrity Certificate and VAPT Clearance must be submitted, duly certified by OEM to the Bank for sign off of successful installation.
- 10) Post implementation of the solution, the scope contains support for the following activities, but not limited to, from time to time, in relation to maintenance and upgrades/updates/patches : (a) Firmware Upgrades, (b) Faulty Parts replacement, (c) Hardware System monitoring, (d) Troubleshooting & Performance Tuning, (e) Operating System Upgrades, (f) Upgrades of supplied software, (g) Advisories on software upgrades & vulnerabilities, (h) Support during DR Drills, (i) OS Administration & patching as per OEM guidelines (j) Any support required to make systems & software up and running.

Note – The list mentioned above is the indicative list, however the successful bidder should provide end-to-end support and repair for any activities and resolution of any issues related to new deployment without any extra cost to the Bank.

- 11) The patches (critical / non-critical) as and when released by OEM, for the proposed solution/ servers/OS , to be tested first in test environment, and thereafter deployed, installed and configured by bidder's team at bank's site, as per Bank's requirement during the contract period without any additional cost to Bank.

- 12) The bidder has to provide a certificate, on OEM's letter head for upgrade and uninterrupted maintenance support for period of five (5) years.
- 13) Post installation of Solution with all its component including OS, VA & PT (Vulnerability Assessment & Penetration Testing) shall be conducted and report will be provided by Bank Info Sec Team to bidder. All findings/issues pointed out in the report to be complied/fixed before installation of the software (Database, application). Moreover, periodic review audit of the database and application is conducted by Information Security and other authorities on the installed components, and its report including VAPT Reports to be complied by bidder/OEM within the timelines, during the entire period of contract.
- 14) The Bidder should provide changes (updates) and upgrades (including version upgrade) with regard to changes in regulatory/statutory/governing bodies' requirements at the earliest (to complete the activity before the deadline set by the authority) and free of cost during the contract period.
- 15) The Bidder should provide and implement functionality changes as required by the end user during the contract period.
- 16) The Bidder shall mandatorily comply with the service Level /High availability and Uptime requirements. For the complying the same, if bidder has to deploy/engage additional resources shall be included in the offer/price schedule itself. No additional cost shall be entertained for matching the SLA/Uptime requirement as asked in the RFP for contract period.
- 17) The Bank as its discretion, reserves the right to shift the equipment (the solution) to a new location during the contract period (within Data Centre or outside Data Centre) depending upon the requirement. Accordingly, the bidder will arrange to shift the same and install and commission at new location without any additional cost to the Bank.
- 18) The bidder shall provide clear requirement for Bank's provided infrastructure. Any additional/change in requirement regarding Bank provided infrastructure will not be entertained by the Bank after awarding the contract. The Bidder shall be responsible for delivering the same. The integration with Bank's existing and future tools will be responsibility of bidder without any additional cost to the Bank. In case, if any OEM can't integrate with third party monitoring tool for OEM product, then the

bidder need to be bundle OEM tool in his response to the bid. (Performance, Availability, Patching, Monitoring, Dashboard with Graphical representation)

- 19) If the solution is not performing as per specifications/scope in this RFP, bidder shall upgrade/enhance the solutions / devices or place additional devices and reconfigure the system without any extra cost to the bank to match the scope and SLA
- 20) The Contract Term / Project period to be considered as 5 years from the starting of the contract i.e. **date of Implementation of central setup at DC and DR (in high availability and redundancy) and installation/availability of solution at minimum 10 % of ordered endpoint or minimum 1000 nodes/ end points of the Bank/Branches whichever is higher for each solution with all enabled features as per RFP.** The central setup shall be implemented as asked in sizing of the solution and shall ensure high availability and redundancy to achieve the scope and SLA. The setup should have augmentation capacity to cater the future requirements.
- 21) The solutions pending for sign-off beyond Implementation period will attract penalty for implementation delay. If reason for delays are not attributable to the Bidder, such cases may be suitably considered on case to case basis by the Bank on its sole discretion. The Bank may ask for extension of contract on same terms and commercials for required solutions for further period (minimum One Year) or its EOS/EOL date.
- 22) As the late sign-off of any solution may impact the Warranty / AMC timelines under back-to back agreements of SI with OEM, they are advised to take care of the same in their agreements with OEMs. The Bank will not consider any request for adjustments in such cases and will seek full five year active life of each solution with full OEM support & services after acceptance and starting date of solution in the Bank's environment.
- 23) Each solution's initial and Additional license requirements, High Availability /DR infrastructure, storage requirements and other information is captured in Part 5 : Technical Specifications & Sizing.
- 24) The services/ solutions offered should be modular, scalable both horizontally & vertically, and should be able to address Bank's requirements during the period of contract and even beyond future license figures given.

- 25) All the Hardware & Software supplied under this contract should be IPV6 & TLS 1.3 or higher Ready. Bidder to provide requirement explicitly for VM and Storage infrastructure required for implementation of each solution. The change in requirement at later stage may affect the project and its timelines. The bidder shall own the responsibility for any such delay.
- 26) The services/ solutions in scope should be designed with adequate redundancy and fault tolerance to meet the Business Continuity requirements/BCP plan of the Bank.
- 27) The services / solutions offered should not have any significant adverse impact on the existing infrastructure/ business of the Bank neither during installation nor during operations. There should be no service disruption as part of implementation or any upgrades. Any such incident may attract penalties as per SLA.
- 28) The services/ solutions offered should not require any major Network Architecture change in existing Network Architecture or existing device replacement on the part of the Bank Except Following
 - i. There are some solutions which will be in line and need architecture and data flow reroute changes without which the solutions cannot be deployed.
 - ii. Port mirroring for solution which work on Mirror traffic.
- 29) Bank will provide VM Infrastructure (Virtual Machine Servers and Window OS), Database only Oracle / SQL Server (in case, proposed database by bidder is not Oracle/ SQL Server, bidder shall provide the same with maintenance for entire contract period) for all security solutions except Proxy solution, in which the bidder shall require to provide all kind of Hardware, OS, DB and related infrastructure for deployment of Proxy solution at DC, DR and BKC.
- 30) Bidder shall quote necessary infrastructure/ appliances if required extra to match the solution as per bank's RFP requirements. The Solution should be able to keep one year data online while backup of older data more than one year till ten years shall be backed up using Banks existing backup solution with solution's application, and restorable whenever required by solution's application.
- 31) For appliance based solution by following compatibility needs to be ensured by the Bidders related to Backup requirement.
- 32) The bidder has to integrate all components/ servers procured under this RFP, with existing Backup infrastructure of the Bank. The Bank is using Cisco MDS 9148S

SAN switch through which Backup infrastructure is connected. The bidder has to assess & procure the required port license as well as SFP module for integration with SAN switch. The Bank is having NEO (OV-NEOs-T48) Tape library and Commvault 11 as Backup software. The Bidder shall provide final VM Requirement as part of technical bid/solution design document as mentioned above. The VM requirement shall be verified in Technical Evaluation phase.

- 33) For VMs, Bank will provide Hardware infrastructure (Storage/ RAM/ Microsoft operating system (OS)) and Oracle Database licenses/ SQL Server Database licenses (except Proxy solution, in which the bidder is required to provide all kind of Hardware, OS and related infrastructure for deployment of Proxy solution). The bidder shall depute the qualified experienced professionals from OEM/bidder's solution team for troubleshooting and necessary installation and configuration of Operating System and Database for installation of procured solutions in Bank's VM Infrastructure / private cloud including SCD preparation and VA PT compliance of each components.
- 34) In case, bidder propose to deploy the solutions on any other database (except Oracle / SQL Server), then the bidder shall include the same in the quoted price as per price schedule during submission of the bid.
- 35) All solutions proposed should be leader/challengers in the leading industry reports like Gartner's Quadrants. The Latest available reports will be used as reference. If for any solution, Gartner's reports are not available, the Product categorized as Leaders as per other leading industry reports can be considered. All solutions proposed must have a post- sales OEM production/Enterprise category support through established service centres / offices preferably within India. Successful bidder has to submit a copy of such support availed by them from OEM to the Bank. The bidder needs to comply as per eligibility criteria i.e. Format 6.16.
- 36) The proposed solution should be latest one and matching the current security and statutory requirements and should not be end of life or end of sale and the OEM should guarantee that the solution support will be provided for a minimum of 5 years by the OEM from the date of purchase order / date of first deployment, with extendable up to minimum 1 year or up to EOS/EOL on same terms and conditions. If any of the solution is declared end of life/end of support by the OEM during period of contract, the bidder/OEM shall provide its new version to the Bank without any extra cost to the bank for rest of the contract period and extendable to minimum 1 year on same terms and conditions.

- 37) The Bank has a complex and large infrastructure with multiple resources maintained and managed through multiple vendors. So for seamless implementation close coordination is mandatorily required with other vendors/asset owners and bank personnel. A robust documentation system needs to be in place for all to understand the process and their responsibilities. The bidder needs to perform the documentation from Day-1 (having all details i.e. of all configurations, support mechanism and architecture of deployment) and same to be shared with Bank's team.
- 38) The bidder/ SI shall Work in Liaison with various service providers/ departments/divisions of the Bank, existing application vendors of the Bank for training/ integration of services/ solutions with existing application platforms, servers, security devices, storage environments, network, and security solutions.
- 39) The proposed solutions should provide dashboard view for the various level of users / department heads as per Bank's requirement.

Creation of dashboard with the following features-

- Top Management View (Board) – Having Summarized view of various department (Can be explored to show the detailed information pertaining to the particular / all departments (individually)).
 - Department Heads (Various IT Business Department Heads) – Having detailed information pertaining to a particular department. The department head can have access to information pertaining to their department only. However, being common department head, the head may have access to the information pertaining to more than one department.
 - CISO (complete and detailed dashboard of each security solutions of the organization)
 - System Administrator (for the systems associated with this administrator)
 - Network / Security Administrator (for devices / equipment for which he is administrator)
- 40) The bidders shall also provide the following OEM certified documents as part of the deliverables of the project.
- Original manuals of all proposed hardware/software/applications
 - Standard Operating Procedures
 - Installation & Configuration Documents (along with parameters)

- Network & Security Design Documents (Will be approved by the Bank)
 - Troubleshooting Manual
 - Executive summary report for the project to the management
 - Functional and operational requirements
 - Project design/plan
 - Product description
 - Guidance for best practices, implementation guidelines
 - User acceptance test plan, if any
 - Training materials
 - Quarterly health check-up by OEM (Frequency of health check-up be changed for compliance of regulators/ RBI) and compliance of observations (if any) by bidder/OEM. (Will serve as mandatory compliance for release of quarterly payment).
 - All the above documents (soft copy or hard copy) should be provided by the SI, vetted by the bank, suggestions incorporated by Bank and SI and then provided to the Bank.
- 41) The OEM should submit the undertaking regarding SAST/DAST and Application security testing done through established authorized partner/ companies/vendor or consultants. The bidder should submit all compliance reports along with technical bid.
- 42) The bidder shall submit the software/solution integrity certificate as per format 6.26.

3.3.2 Training:

- i. The Bidders shall provide professional training by OEM or its Certified Training partner to the identified Bank personnel / team (minimum 5 in number) on each solution (for minimum 3 days) for features / service architecture, and functionality during and after implementation. As all solutions required in this RFP are dynamic and critical in nature & may undergo changes in future (in compliance of RBI guidelines), therefore additional trainings at the gap of 2 years (after go-live) to be provided to Bank's personnel (minimum 5 in number) for each solutions i.e. in 2nd year and 4th year. The related certification should also be awarded to the trainees who undergo the training and exam thereafter for the each solution. The

bidder shall arrange all end to end expenses till attaining the certification by the trainee without any extra cost to Bank.

- ii. The Bidders shall also arrange the Certification “Certified Information System Security Professional -CISSP” and training of requisite days to Bank Team – Total 10 Nos. (05 Nos. in first year and 05 Nos. in third year (first quarter of third year)) during currency of the contract. The year of training and count may be subjected to change with upper limit on count i.e. 10 Nos. All related arrangements (including exam cost and its renewals up to 5th year i.e. end of contract) shall be done by the bidder till the possession of certificate by the Bank’s personnel without any extra cost to the Bank.
- iii. The solution should be demonstrated to the IT Department & Information Security Cell staff of the Bank after completion of the implementation in test environment. The feedback as suggested by Bank/Info Sec Team, must be incorporated in the solution by the bidder and thereafter tested first in UAT environment and clearance shall also be obtained from Bank’s/ Info Sec team before Go-live into production environment. **The bidder is to ensure that no pendency of any VA & PT (Vulnerability Assessment & Penetration Testing) point before deployment in production (if available, needs to fix by bidder). No additional cost will be paid by Bank for the same.**

3.3.3 Implementation & Ongoing Compliance Requirements

For the purpose of implementation, the following points should be noted:

- i. The Bank will provide VM Infrastructure and storage for all security solutions. Bidder has to quote the additional/ necessary appliances (if required extra) to match the solution as per bank’s RFP requirements.
- ii. The solution, services, software and all other necessary items would be provided by the Bidder. Only VM infra & Windows Server OS will be provided by the Bank as cited above (Excluding proxy solution which is appliance based).
- iii. The Bidder shall provide requirement explicitly for VM infrastructure required for implementation of each solution. The change in requirement at later stage may affect the project timelines. The bidder has to own the same and ensure coordination to avoid the same.
- iv. Passive Cabling (if required) to make the solution workable at DC and DR shall be done by the bidder. The bidder should do the site survey for the same.

- v. The bidder has to integrate deployed solution with existing security tools deployed by Bank.
- vi. All Software / Databases deployed as part of solution at Bank under scope of this RFP should be licensed with back-to-back support contracts from respective OEMs for the contract period. The licenses should be in the name of Bank of India or specifically purchased for bank with Bank's name mentioned in license & copies of these should be submitted to Bank. (The owner of licenses will be Bank of India, even after expiry of the contract since the licenses are perpetual).
- vii. Bidder should supply products as specified, and Services which includes Implementation, Integration, management, maintenance, audit compliance and knowledge transfer in respect of their solutions as detailed in the subsequent sections.

3.3.4 Implementation Planning:

- i. The Bidder, in coordination with OEM shall do analysis and submit a detailed study of the Bank's infrastructure and requirements, road map mentioning all the pre-requisites, time-frame of mile-stones/ achievements leading to the full operationalization of the solution vis-à-vis Bank's requirement.
- ii. The Bidder shall submit project plan, get it approved by the Bank and implement the project based on timelines. The Breach of timelines will attract penalties mentioned in Liquidated Damages/ Service level Agreement section of RFP.
- iii. The bidder shall adopt industry best practices related to information security in solution design which must be in compliance of RBI guidelines. The information security clearance for each solution has to be obtained by the bidder from bank's CISO as per Bank's CISP Policy before moving the solution to UAT and in production. Any issues related to security clearance needs to be complied by the bidder, in time bound manner, to enable the solution to move to UAT (and thereafter in production) considering the date of installation as per the RFP.
- iv. All Solution's Architecture, deployment methodology & configurations parameters at the Bank end to be certified by OEM mandatorily, for any Sign-Off from Bank's end

3.3.5 Implementation:

- i. The bidder/ SI will perform commissioning, implementation and configuration of delivered products/ solutions as per RFP, inline to best industry standards and statutory compliance. In case of delay / default in installation of delivered Product/software (solution) by the bidder or if bidder fails, the OEM shall do the implementation of entire solution directly for timely implementation completion of project. Any additional charges, if sought by OEM for engagement, to be borne by the bidder.
- ii. The bidder shall submit undertaking for each solution from OEM regarding its expertise in implementation of all solutions as proposed in the RFP, to be submitted by the bidder as per format 6.24. The undertaking for each solution has to be submitted by the bidder separately for all offered products.

3.3.6 Ongoing Compliance & Improvement

- i. The Bidder would be responsible for updates, upgrades, patches, bug fixes, version upgrades for the entire solution (and/or its part thereof) during the period of the contract, warranty and AMC. The OEM support for major upgrades if required should be factored in project cost itself.
- ii. In addition to Operations Management of their own solutions, the on-site team will be responsible for closure of findings of VAPT and SCD review conducted by the Bank on underlying infrastructure and assets of these solutions.
- iii. The Bidder should keep on improving the policies configured on an on-going basis for each solution.
- iv. The Bidder shall be responsible for all technical support to maintain the required uptime. The Bidder shall be the single point of contact. Bidder should have back-to-back support with OEM during the total contract period for necessary support. The end-to-end deployment (from bidder's side) i.e. installation, configuration and integration to be performed by bidder in coordination with OEM. To complete all activities as per the RFP terms, any support (if required) from OEM shall be arranged and ensured by bidder on immediate basis.
- v. Bank may request Bidders for demo or to conduct POC of any/all security solutions without any extra cost to the Bank.

- vi. The Bidder shall ensure the proactive monitoring of the solution to ensure high availability and match the SLA of the solution. The bidder shall fulfill all reporting requirements of the Bank.
- vii. The project shall be subjected to audit from Bank and/or third party and/or regulatory bodies. The bidder shall be responsible to co-operate and provide necessary information and support to the auditors in time bound manner (as per the auditor's timelines). The Bidder must ensure that the audit observations are closed on top priority and to the satisfaction of the Bank, regulator and its appointed auditors. Extreme care should be taken by the Bidder to ensure that the observations do not get repeated in subsequent audits. The repetition of non-compliance of any observations shall be treated as non-adherence of SLA and shall attract penalty as per SLA Clause. The bidder shall ensure to mitigate vulnerabilities as per advisories issued by Government Authorities / Statutory bodies in India and abroad.
- viii. The Compliance to various audits like ISO 27001:2013 PCI DSS, ISO 22301 etc., shall be arranged and ensured by the Bidder.

3.3.7 Contract Expiry / Termination:

- i. 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 person of the bank (or) to a third party nominated by the Bank.
- ii. In case of termination of contract / end of contract period, Bidder has to provide extended services till supply of next solution or till next one year or as per Bank's intimation after contract whichever is decided by the Bank, with same terms and conditions as per SLA. In such case bidder to ensure that all the solutions are up to date with latest technological innovations and in compliance of existing terms and conditions of the RFP. In case of violation of SLA terms, Bank's at its discretion reserves the right to invoke the PBG (Performance Bank Guarantee).

3.3.8 Sizing & Scope of Work for each solution

- i. Each solution's initial and future license requirements, HA/DR infrastructure, storage requirements and other information is captured in Part 5 Technical Specifications.

- ii. Each solution shall be deployed in high availability and Redundancy at Bank's DC and DR each.
- iii. The Sizing of each Solution should be done on the basis of Initial license requirements given by the Bank. The Active life period shall be of 5 years for each solution from start date of the same in the Bank's Setup. The same solution should be scalable to cater additional licenses requirements without any disruption of existing setup / zero downtime.
- iv. The Bidder shall ensure that any additional hardware/ software/ network equipment required to operationalize the respective solutions/ devices must be provisioned by the Bidder while proposing the Solutions to the Bank and their details should be given in the technical and commercial bill of material.
- v. If the same is not ensured, the Bidder shall be responsible to provide such hardware/ software/ networking equipment free of cost to the bank at the time of implementation.
- vi. The services/ solutions offered should be modular, scalable both horizontally & vertically, and should be able to address Bank's requirements during the period of contract even beyond future license figures given.
- vii. The Bank may ask the Bidder to provide calculations/ logic arrived at the sizing for all appliances/ hardware as part of the response.

3.3.9 Annual Maintenance/Technical Support Contract

- i. All the equipment / Solutions i.e. All the parts/ components (tangible/ in-tangible) of deployed both hardware and software (any other software provided under this contract) would be covered under comprehensive warranty with ATS for a **period of one year** and thereafter comprehensive AMC (for hardware) and ATS (for software) for 4 years. In total, the contract period shall be of 5 years.
- ii. ATS/Warranty will commence from the acceptance date / Sign-Off Date by the Bank for each solution. The start date shall be of Go Live date.
- iii. If there is any gap between Bank's requirement and OEM warranty/AMC/ATS, then it will be the responsibility of bidder to fill up the gap without any additional cost to the bank.

- iv. The bidder should install only licensed version of any software. License should be in the name of Bank of India. Necessary CD/ URL for download to be provided for future purpose.
- v. The ATS/ warranty and/or its AMC, covers all updates and upgrades during contract period of 5 years.
- vi. The bidder shall be responsible and work as asset owner for the allotted VM and other infrastructure provided by the Bank. The necessary maintenance should be carried out by the bidder in coordination with VM and other service Provider of the Bank. The Bidder shall ensure, OS Upgrade/ bug fixes, Server patching as required by Bank's SOC advisory for the allotted infrastructure.
- vii. The Bidder shall be responsible for all technical support to maintain the required uptime. The Bidder should have necessary back-to-back support agreements with the OEMs for all the required onsite support for entire project period.
- viii. During warranty/ AMC/ ATS period, the scope includes resolving supplied hardware and software related issues, including installation/reinstallation of OS and of any other software supplied by the bidder, due to any reason whatsoever for the above mentioned hardware and software, without any additional cost to the Bank.
- ix. The bidder should only deploy well-experienced professionals during deployment, warranty and post warranty period.
- x. The Supplier shall warrant that the products supplied under the Contract are of the most recent version/latest and that they incorporate all recent improvements in design and / or features. The Supplier shall further warrant that all the Products supplied under this Contract shall have no defect, arising from design or from any act of omission of the Supplier that may develop under normal use of the supplied products in the conditions prevailing in India. Professionally qualified personnel, who have expertise in system software supplied by the vendor, will provide these services.
- xi. The Supplier shall comply with the performance guarantees specified under the Contract. If, for reasons attributable to the Supplier, these guarantees are not attained in whole or in part, the Supplier shall make such changes, modifications and / or additions to the Products or any part thereof as may be necessary in order to attain the contractual guarantees specified in the Contract at its own cost and expense and to carry out further performance tests.

- xii. Upon receipt of such notice, the Supplier shall with adequate speed, repair or replace the defective products or part thereof without cost to the Bank.
- xiii. If the Supplier, having been notified, fails to remedy the defect(s) within the 4 hours' time duration from the incident, the Bank may proceed to take such remedial action as may be necessary, at the Supplier's risk and expense and without prejudice to any other rights, which the Bank may have against the supplier under the Contract. The Bank shall also impose penalty as mentioned in clause for such defects in the solution as per clause 4.18.
- xiv. During Support Period, Supplier guarantees an Uptime of 99.90 % on monthly basis for the entire/core solution proposed. Please refer to **Clause 4.18** for details of uptime required by the Bank.
- xv. The bidder shall ensure re-deployment of software/solution or its agents/scripts at central or remote sites or at endpoints as part of maintenance only. There shall be no additional charges payable for re-designing / re-deployment of solution at any or all additional endpoints including DC and DR sites of the Bank. All activities pertaining to continuity of the solution shall be ensured by the bidder as part of warranty and/or AMC without any extra cost to the Bank.
- xvi. During warranty and ATS period, the support should be of Highest / Enterprise support level. For Highest Priority Calls (P1 – Calls), response to be provided by OEM within 15 minutes. The Expected resolution Time for any call should not go beyond 4 hours (maximum).
- xvii. If the solution/ product is termed faulty/ non-operational, the upgrade/ replacement (with new one) should take place on immediate basis, not more than 4 hours considering the criticality of the business requirements of the Bank.
- xviii. The warranty and AMC/ATS will cover every kind of repair and support including technical on-site support from the Bidder and back to back OEM support for software updates, OS upgrades, version upgrades, troubleshooting, TAC support from the OEM, hardware replacement, hardware upgrades, and all relevant updates for any or all modules procured as part of this RFP to ensure that the most updated security risk library is available to the Bank at any given point in time for entire contract period.
- xix. During the warranty and AMC/ATS period, the Bidder will have to undertake comprehensive onsite maintenance as per defined frequency, support for proper operation, performance and output as specified in Part 5- technical

specifications of the all the networking and security equipment supplied by the Bidder.

- xx. During the warranty and AMC period, the Bidder should maintain the acceptance criteria and shall be responsible for all costs relating to service, maintenance (preventive and corrective), technical support and transport charges from and to the sites in connection with the maintenance of the solution or any components/ parts there under, which, under normal and proper use and maintenance thereof, proves defective in design, material or workmanship or fails to conform to the specifications, as specified.
- xxi. The successful Bidder shall ensure that services of professionally qualified persons will be available for comprehensive on-site maintenance of the equipment during warranty/AMC period.
- xxii. BOI reserves the right to go with any other Bidder for AMC during AMC period if Bank finds that the services provided by the bidder are not satisfactory.
- xxiii. The selected bidder shall provide comprehensive AMC for all the equipment / Solutions that are delivered & installed at Bank's sites for a period of four year after expiry of warranty period of one year.
- xxiv. If Bank decides to avail one year additional support for some /all solutions, their AMC Contracts shall be extended accordingly by Bidder on same terms and conditions.

3.3.10 Scope of Facility Management Services

3.3.10.1 Operation's Phase

3.3.10.1.1 General Scope

- As part of Operations Phase, OEM has to conduct quarterly health check and preventive maintenance to ensure industry best practices are followed and submit a report for the same to the Bank. Any observation to be complied by the bidder in time bound manner to meet the SLA.
- Operation team and Project Management/Implementation/Roll out team should be separate
- Operations phase should begin once implementation of the solution has fully completed and acceptance/sign-off has been received from the bank.

- The bank requires 24X7X365 operation with equal efficiency.
- Company has to provide background verification certificate before deploying the resources.
- The Police verification (PV) certificate (issued within six month of joining) should also be provided by bidder for all the resources deployed onsite at Bank with in a period of one month. The police verification request/ application to respective government authority must be submitted within one week of joining.

Table-1 Onsite Manpower Required (In total for all solutions):

• Type	• Quantity
• L1 : 24 x7 x 365 (366 in leap year) onsite	• 2 manpower per shift
• L2 : 24 x7 x 365 (366 in leap year) onsite	• 1 manpower per shift
• In Addition of above, L2: • Bank's Business Hrs, (10 AM to 6 PM) (All 365 days (366 in leap year))	• 2 manpower
• L3 : General Shift (OEM only) (All 365 days (366 in leap year))	• 1 manpower As per Bank Working Days. (Monday to Saturday except Second and Forth Saturday) and during any activity and issues reported. (1 resource / day)

- In case of exigency, support arrangement should be available during off-hours as a part of the crisis / incident management process.
- **The Bidder shall provide Shift Roster and calculation to justify provided resources count as part of Technical bid submission. In case Bidder fails to provide the justification acceptable to Bank, the Bid may be rejected.**
- **In case of discrepancy found in Shift Roster during deployment of manpower, Bank will deduct the amount on pro-data basis for said manpower count.**
- **Buffer arrangement:** The bidder will maintain enough provisions of additional manpower for managing the absence of any resources due to whatsoever reasons. (Like company policy, work-hour limitations, leave, sickness, recess, interval, training, etc.)
- The Bidder should share details and explanations as to the number of manpower they would provision for the services with Technical Evaluation documents. They will have to justify it to the evaluation team during the presentation phase.

- The Successful Bidder shall deploy their own pay-roll employees' On-Site Bank of India for all i.e. L1, L2 & L3 Level employees, undertaking from company to be submitted. No outsourced / sub-contracted staff to be deployed during any phase of the project (entire contract period)

3.3.10.1.2 The Onsite Resource Qualifications:

Type of Engineer	Educational Qualification
L1	Should be Science Graduate (IT / Computer), preferably, BE/B. Tech/MCA with minimum 2 years of relevant and 3 years of total experience in the field of IT Security and implementation/support of in-scope solutions Should be certified with at least 1 certification out of the following: CEH CCNA/CCSA/RHEL/MCSA/UNIX OEM certification for the solutions part of this RFP
L2	Should be Science Graduate (IT / Computer), preferably, BE/B.Tech/MCA with minimum 3 years of relevant and 5 year total experience in the field of IT Security and implementation /support of in-scope solutions Should be certified with at least 2 certification out of the following: CEH/ CISA/CISM/ISO 27001 CCNA/RHEL/MCSA/UNIX OEM certification for the solutions part of this RFP
L3	Should be Science Graduate (IT / Computer), preferably, BE/B.Tech/MCA with minimum 5 years of relevant and 7 years total experience in the field of IT Security and implementation /support of in-scope solutions Should be certified with at least 2 certification out of the following: CEH/ CISA/CISM/ISO 27001 CCNA/RHEL/MCSA/UNIX OEM certification for the solutions part of this RFP

3.3.10.1.3 Team Members and Their Roles & Responsibilities

➤ Account Manager

- i. A senior management member from the Bidder shall be identified as the project single point of contact acting as Account Manager; her or his responsibilities are outlined below:
- ii. Primarily accountable for successful operations of the project across Bank
- iii. Act to remove critical project bottlenecks
- iv. Identification of working team members, team leads etc.
- v. Single point of contact for Bank's senior management

➤ Technical Service Delivery Manager (L3)

- i. One Dedicated Onsite Technical Delivery Manager will be placed by the Bidder at the Bank's Site to ensure service delivery levels are as per SLA requirements
- ii. Monitor operations for all solutions implemented at Bank
- iii. Help Team Leads in resolving technical issues & coordinating with OEM as escalation follow-up for long pending Tickets & calls
- iv. Co-ordinate with all stake-holders
- v. Monitor quality and risk related activities
- vi. Identify and implement best practices during project operations at Bank
- vii. Periodic reporting to Bank on the status, issues/ challenges faced and how these are handled

➤ Team Leads (L2)

- i. Lead daily Operation efforts, Report on progress to Technical Delivery Manager and Bank
- ii. Help Operation Team (L1) in resolving technical issues & coordinating with OEM as escalation follow-up for long pending & calls
- iii. Co-ordinate with all Teams for follow-up for open tickets & activities
- iv. Do Server patching / hardening & VA/PT on solutions under their preview
- v. Do periodic preventive health check / Version Upgrade for solutions under their preview
- vi. Monitor quality and risk related activities on solutions under their preview
- vii. Identify and implement best practices / Configurations on solutions under their preview

➤ Working Team (L1)

- i. Have daily Operation efforts, Server / Solution Dash board Monitoring, Attending user calls, opening tickets etc. and report on progress to Team Leads
- ii. Resolving technical issues & lodge tickets with OEM, have follow-up for long pending calls

- iii. Co-ordinate with all Teams for follow-up for open tickets & activities
- iv. Do Server patching / hardening & VA/PT on solutions under their preview
- v. Do periodic preventive health check / Version Upgrade for solutions under their preview

➤ **Technical Account Manager (TAM)**

- i. A senior management member from the **OEM** shall be identified as the Technical Account Manager for each solution; her or his responsibilities are outlined below:
- ii. Primarily accountable for issues not resolved by On site resources as well as L2 & L3
- iii. Act to remove critical project bottleneck by connecting Bank staff with the Technical team of OEM
- iv. Single point of contact for Bank's senior management from OEM side.
- v. The bidder shall share TAM detail for each solution.
- vi. The monthly review meeting shall be arranged with Account executive, TAM and higher operations leads.

3.3.10.2 Implementation Phase

- i. All team resources included in implementation should be on the payroll of Bidder or OEM.
- ii. The Bidder/ OEMs shall provide on-site resources at bank's central locations for implementation of their respective solutions during the implementation phase. In case the Bidder is not able to resolve the Bank's queries or delays the implementation beyond stipulated timelines, the OEM shall ensure implementation with no extra cost to the Bank. Hence it is expected to work hand in hand by both parties i.e. bidder as well as OEM for implementation and operation phase.
- iii. Subcontracting: Subcontracting is not permitted in any manner in entire contract period.
- iv. The implementation team should be different from regular resources (used in operations phase).
- v. Separate implementation team to be deployed by bidder for each solution, to have parallel implementation of all solutions. This is also required to avoid overlapping of resources engaged for common implementation.

3.3.10.2.1 Bidder' Project Team Members and Their Roles & Responsibilities

➤ Project Sponsor

A senior management member from the Bidder shall be identified as the project single point of contact acting as Project Sponsor. His/her responsibilities are outlined below:

- i. Primarily accountable for successful implementation of the project across Bank
- ii. Act to remove critical project bottlenecks
- iii. Identification of working team members, project management office members and team leads
- iv. Single point of contact for Bank's senior management
- v. The project sponsor shall be part of steering committee for implementation at Bank

➤ Project Manager

One Dedicated Project Manager will be assigned by the Bidder at the Bank's Site to ensure implementation timelines are met to achieve desired results. His/her responsibilities are outlined below:

- i. Monitor Project implementation at Bank
- ii. Co-ordinate with all stakeholders
- iii. Monitor quality and risk related activities
- iv. Identify and implement best practices during project deployment at Bank
- v. Periodic reporting to Bank on the status, issues/ challenges faced and how these are handled

➤ Team Leads

- i. Lead daily implementation efforts
- ii. Report the progress to Project Manager and Bank
- iii. Identify and report any risks to Project Manager and Bank
- iv. Seek advice from the Project Manager on mitigation measures for the Bank

➤ Working Team

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

3.3.10.2.2 OEM Team

During implementation phase, OEM resources shall be available at DC/DR deployment location for finalizing the design and implementation plan of their respective solutions for:

- i. Training on functionality of the solution to Bank's designated team / departments / division

- ii. Validation of solution design and architecture as prepared by bidder as per Bank's requirement
- iii. Continuous monitoring of implementation at each location
- iv. Provide SME support to working teams during implementation and operations
- v. Ensure customization is in line with Bank's requirements
- vi. OEM Certification of Deployed Architecture & Configurations done at Bank of India Setup is necessary after implementation of its products for Bank Sign-Off
- vii. Quarterly health check-up of the solutions implemented by the bidder

If the OEM/Bidder implements some solution through a partner of OEM, that partner should have prior implementation experience at more than one organizations in India for similar size deployments.

3.3.10.3 Other Terms & Conditions - Facility Management services includes but not limited to the following:

1. Implementation, roll out and maintenance of all the solution to all end points.
2. Overall proactive monitoring through online dashboard and management of equipment's, endpoints and related services on all sites under this RFP. The implementation of solutions on additional agents after signoff of the solution shall be done by onsite FMS without any extra cost to the Bank.
3. The Online Dashboard/Tool (Centralized Monitoring Tool) (integrated with existing infrastructure of the Bank) shall be available from the starting of project i.e. from deployment of first solution on first node itself. The scope of FMS shall only be completed on availability of dashboard tool/monitoring Console since starting date of the project and payment of FMS shall also be subjected to availability of Monitoring dashboard / Console system as per project.
4. Overall monitoring and management of the project during and post installation for the full period of contract.
5. Coordination for delivery/ deployment/discovery of agents/endpoints and Installation of new hardware, software and necessary licenses in stipulated time frame.
6. Quality service delivery to match the uptime /SLA.
7. Onsite team management and proactive response and immediate remedial measures.

8. SLA Maintenance / Management, monthly Uptime reports, utilization reports & interface utilization / reporting of all the devices.
9. Submission of periodical reports on the performance of the equipment's and its reviews. Preparation and submission of other MIS related work assigned by Bank.
10. Redesigning of the solution for optimal output of the solution in interest of the Bank.
11. Crisis Management and Emergency response Procedures
12. The cost of the resources as provided in the Final Commercial Bill of Materials shall be considered as final for the term of the project.
13. The Bank may procure additional resources at the same costs as per need during currency of the Contract. The Bank may also reduce the manpower requirements during the project duration if workloads reduce due to any reason.
14. Before deployment of any resource, his/her profile will be shared with the bank with required CV's and supporting papers to establish conformity with SLA terms. The Bank will have the Interview of the resources before deployment & will give acceptance for deployment based on Interview assessments.
15. It will be bidder's responsibility to get the background checks for resources deployed at the Bank's Site.
16. At the time of resource deployment, the Bidder will have to introduce the resources to Bank via formal communication on company letter head. It will be the Bidders responsibility to get their Identity & Address proofs and submit to the Bank. The Bidder will also be required to provide Police verification report for each onsite resource within 2 months.
17. L2 and L3 should be available on all working days and holidays (24*7*365) as well.
18. If a lower level person does not report on duty, then equivalent or higher level person to be deployed in his place and is expected to perform the job of lower level person and payment will be made as per the payment structure of lower level person only. If Bank is not satisfied with the performance of the standby personnel,

Bank may not accept such standby manpower and in such cases replacement resources should be provided on immediate basis.

19. Bank may ask for replacement of any resource at any point of time. Bidder is expected to provide alternate resource within 30 days.
20. **Buffer arrangement:** The selected bidder shall ensure and maintain enough provisions of additional manpower for managing the absence of any resources due to whatsoever reasons. (Like company policy, work-hour limitations, leave, sickness, recess, interval, training, etc.). The bank shall pay the count of onsite resources (operation phase only) as asked above.
21. In case of exigency, support arrangement should be available during off-hours as a part of the crisis / incident management process.
22. Co-ordinate with all Teams for follow-up for open tickets & activities.
23. The FMS shall do periodic preventive health check / Version Upgrade for solutions under their preview.
24. The FMS Team shall resolve technical issues & lodge tickets with OEM, have follow-up for long pending calls.
25. The Bidder/FMS Team shall identify and implement best practices / configurations on solutions under their preview.
26. The Bank may also reduce the manpower requirements during the project duration if workloads reduce due to any reason. No payment for such reduction in manpower will be paid by the bank.
27. The onsite FMS resources should be prepared to work for extended hours in case of need.
28. The onsite FMS resources should abide by timings as revised by the Bank time to time and the roster of onsite FMS team shall be shared with the designated Bank team on daily basis.
29. The members of the on-site team should be provided with mobile phones by the bidder and the details like Name, Address (Inclusive of Residential Telephone Number), Mobile Number should be provided to Bank.

30. The bidder shall ensure police verification of deputed resources for access in NOC/ SOC (A copy of the same should be submitted to the Bank). Name of emergency contact personnel with relationship and Telephone number should be provided to Bank.
31. Disability if any or suffering for any disease should be informed to the Bank in advance. The bank shall not be responsible for any such disability/disease or physical fitness of the resources deployed onsite, the bidder shall ensure necessary steps for the same without hampering services to the Bank.
32. The on-site team shall maintain attendance register and the same should be shared with Bank on daily/monthly or on defined frequency by the Bank. The bidder shall ensure verification of attendance by Bank's Team on weekly basis. Only verified attendance shall be counted for payment. The bidder shall also submit collated excel sheet of verified attendance to bank's team on monthly basis.
33. The on-site team shall not be changed without prior approval from Bank and adequate notice (minimum one month for Level 1 (L1), two months for Level 2 (L2) and three months for TL/Level 3). Any resigned resource of on-site team should not be relieved before giving suitable replacement, handover and serving required notice period.
34. The bidder shall also provide suitable additional on-site technical staff to supplement the efforts of the on-site support resources during emergencies / contingencies during impact on the systems, Systems and services covered under this scope.
35. Bidder shall provide backup resource in case any of the onsite FMS resource avails leave, however bidder service delivery team will be entirely responsible for team deployment, SLA monitoring, task delegation, workload distribution etc.
36. If the engineer is found not qualified / suitable or his performance is not satisfactory, bidder shall have to replace the engineer within 30 days of written e-mail communication from Bank regarding the same.
37. During the contract period, the bidder and its employees shall at all the times comply with & abide by the security policy of the bank in so far as the same may be applicable to or in respect of the works and the provisions of the contract.

38. Bidder will follow and comply with the procedures and policies, applicable to the scope of work mentioned in the RFP, lay down by the Bank vide IS Security Policy from time to time and also extend full cooperation to the auditors designated by Bank.
39. The FMS shall follow non-disclosure agreement (NDA) with Bank meticulously. The Bidder/ onsite FMS resources at bank shall inform Bank about any correspondence with external entities pertaining to any point mentioned in the scope of the work.
40. All the onsite FMS resources deputed at bank should have Police verification report. Bidder needs to submit the Police Verification report (not older than six months) of FMS resources along with all documents at the time of joining the onsite FMS team.
41. Bidder has to ensure the required uptime of 99.90% on monthly basis. If any additional /resources are required to be deployed by the bidder to maintain the uptime of 99.90%, the bidder has to deploy the resources without any extra cost to the Bank.
42. The bidder and FMS team shall be complying all the rules prescribed as per Bank's Resource Policy /or any other policy/process in place. If not complying, bank at its sole discretion may prohibit entry in Bank's premises.
43. Bank at its discretion can terminate the FMS contract in whole or as part thereof with the bidder and discontinue the same without citing any reason by giving 30 days' notice and applicable amount, on pro-rata basis, for the service rendered shall be payable.
44. The scope of FMS is not limited to above only. Bank shall assign any other work based on the related requirement to the FMS.

3.3.11 Insurance

- i. The successful Bidder should obtain the insurance cover for entire product suit supplied for all risks not only up to date of delivery but also six months after that date.
- ii. The cost for the same will be borne by the successful Bidder. Successful bidder has to submit a copy of the insurance document to the Bank.

3.3.12 License Requirements

- i. All the solutions supplied as part of this RFP should be supplied with Enterprise wide License on perpetual licensing model as per sizing requirements. Bank will have the right to use the solutions for the functions provided by the solutions in any manner and for at any branches, offices, subsidiary units, joint ventures, RRBs, irrespective of the geographical location of the devices being delivered, installed, integrated, monitored and managed. Bank will also have a right to relocate any one or all the solutions to different locations.
- ii. All Software, Middleware Licenses should be supplied by the bidder as per solution requirements and individual OEM licensing policies. The Successful bidder will have to certify the adequacy of licenses supplied to Bank and will have to indemnify the Bank in case of any adverse finding during OEM Audits.
- iii. Freeware/Open source solutions (Software's / OS/ Databases) will not be accepted by the Bank.
- iv. Bidder shall provide list of licenses to be procured as part of the commercial bid and also maintain the inventory database of all the licenses and the updates installed.
- v. All Software Licenses should be in the name of the Bank or specifically purchased for the Bank with Bank's name mentioned in license & copies of these should be submitted to Bank.
- vi. Additional infrastructure to be delivered along with future software licenses once bank will issue purchase order for additional Items on the same terms and conditions. The Details of sizing is provided in the Part 5: Sizing requirements so Bidder can propose scalable solution without replacing initial Hardware and Software components.
- vii. Post closure of the contract, the bank will remain legitimate owner of licenses delivered.

3.3.13 Implementation & Integration

- i. The technical specifications required from the solutions are mentioned in Part 5.

- ii. During Implementation, one dedicated On-Site project manager will be deputed by the Bidder at Bank Site to have timely & smooth project rollout/ implementation. The project manager shall report to Bank within 7 days of issuance of Purchase order. The Bidder is required to review the Bank environment and specify information related to infrastructure readiness at the Bank for seamless implementation of the solution. The implementation Project Manager shall submit the project rollout plan of the solution after vetting/validation of the same by the OEM and also present the same in kickoff meeting (within two weeks) with Bank. The kickoff meeting for each solution shall be convened along with OEM and Bank Team.
- iii. The Bank has a complex infrastructure with multiple resources maintained and managed through multiple vendors. So for seamless implementation, bidder is required to coordinate with other vendors and bank personnel.
- iv. It will be the responsibility of the bidder to integrate all existing and all new solutions without any additional cost to the Bank.
- v. Free upgrade should be provided for all solutions if the end of life of proposed version occurs within the period of contract with bank at no extra cost to the bank.
- vi. All the patches/versions/upgrades/updates should be applied as and when released by the OEM in time bound manner. No implementation of patches/versions/upgrades/updates in time bound manner may lead to applicability of SLA as mentioned in clause **4.18**.
- vii. Patches for all vulnerabilities should be installed in time bound manner as per the SLA terms defined in 'Service Level Agreement' to be signed with successful Vendor.
- viii. Integrate each solution with SIEM solution and IT GRC Solution to provide a single view of events generated.
- ix. Bidder/ System integrator is responsible for configuring the solutions as per Secure Configuration Documents (SCD) as per OEM and vetted by Bank's Team. The bidder shall submit SCD, SOP and architecture diagram to bank team during implementation phase.
- x. The bidder shall include an overview or specimen of the processes followed and implemented in peer institutions as mentioned above.

- xi. The bidder shall develop & publish Escalation Matrix proactively over the project period to Bank with details of bidder & OEM Key persons in order to handle Security & other Incidents efficiently.
- xii. OEM/Bidder will share their generalized APIs with the Bank so that existing as well as future solutions can be integrated without any additional cost to the bank.

3.4 Eligibility Criteria

The bidders who fulfill the following criteria are eligible to respond to the RFP. The supporting documents of the all eligibility criteria are required to be submitted by the bidder along with the Technical Bid. The bids who do not fulfill any of the following eligibility criteria are liable to be rejected.

- i. The bidder should be a registered company in India as per Companies Act 1956 / 2013 and must be in existence for the last 5 years on the date of RFP. The Certificate of Incorporation issued by Registrar of Companies along with the copies of Memorandum and Articles of Association are required to be submitted along with the technical bid.
- ii. The Bidder should have minimum annual turnover of **Rs. 200 Crores** in each of last three preceding three (3) financial years from i.e. FY 2016-17, FY 2017-18 and FY 2018-19. The bidder should submit audited financial statements for the respective year(s). The turnover must be the individual company turnover and not that of any group of companies.

Also, the bidder should have a minimum annual turnover of 30 crores or above from Sales/Services/ Maintenance/ Facility Management of similar security solutions in each of the three (3) financial years from i.e. FY 2016-17, FY 2017-18 and FY 2018-19. A self-declaration confirming the same, duly certified by same statutory auditor (who have audited the annual financial statements) to be provided only.

- iii. The Bidder should have net profit in each of last three (3) financial years from i.e. FY 2016-17, FY 2017-18 and FY 2018-19. The bidder should submit audited financial statements for the respective year(s).

- iv. The bidder should be highest / premium level partner of OEMs with an authority to sell, upgrade supply, service and maintenance of the proposed solutions (hardware and/or software) during the entire period of contract with the Bank as on the date of RFP. Relevant Certification to be attached with the bid document.

The Bidder needs to submit Manufacturer Authorization Form (MAF), having reference of this RFP, from respective OEMs stating that bidder is authorized partner/ System Integrator of OEM and is authorized to participate in this RFP.

The bidder must submit letter from OEM confirming the “Back-to-Back” agreement / arrangement for next 5 years to Bank of India, if contract is awarded to the bidder.

- v. During last 5 years, the bidder should have at least 3 years of experience in undertaking continuous **Annual Technical Support** (ATS) of minimum five security solutions in minimum One Bank (Public / Private) / Financial Institutions. Reference letter from such organizations regarding satisfactory services to be provided by them.

For this, the bidder may submit the reference of more than one organizations (having reference of one or more solution implementation) to comply that bidder is having experience of successful deployment and maintenance of all solutions. The bidder is required to submit the individual experience letter with word “satisfactory services” confirming the same. Non-submission of the reference experience letter with word “satisfactory services” will not be considered.

POCs done will not be treated as experience of the Bidder.

- vi. During the last 5 years, the bidder should have **deployed minimum five solutions out of proposed solutions** in Bank (Public / Private) / Financial Institutions, each having minimum business mix of Rs 2 Lakh Crores as on 31.03.2019 with similar setup and DC/DR Architecture. For this, the bidder may submit the reference of more than one organizations (having reference of one or more solution implementation) to comply that bidder is having experience of successful deployment and maintenance of all solutions. The bidder is required to submit the individual experience letter with word “satisfactory services” confirming the same. Non-submission of the

reference experience letter with word “satisfactory services” will not be considered.

- vii. All/ Proposed OEM Product(s) as solutions should have been implemented in Banks (Public / Private) / Financial Institutions each having business mix of minimum Rs. 2 Lakh Crores as on 31.03.2019 and above, earlier in the last 5 years and presently under support.
- viii. In the response to the RFP, both bidders i.e. OEM (in individual capacity) and OEM with SI can't bid simultaneously i.e. **either** the OEM (Original Equipment Manufacturer) in individual capacity **or** OEM with SI i.e. their authorized distributor in India can bid in the RFP.
In case, both OEM (in individual capacity) and OEM with SI submitted the bids, the bid submitted by OEM (in individual capacity) will be considered.
- ix. The bidder/OEM should have experience in **managed security** in Banks/BFSI in India and deployed minimum One SOC in India The bidder should also have own/registered support offices for TAC level Support in Mumbai and Bengaluru for after sales support services and maintenance of proposed solution, hardware and software. List of branch / support offices full details of Name, Contact person, Address / Telephone Numbers should be attached.
- x. The bidder has to submit Integrity Pact (IP) duly signed by authorized signatory as per the format “Format 6.18” mentioned in the RFP, on stamped paper at the time of bid submission. The bid shall be liable for rejection in case of non-submission of IP.
- xi. The Bidder should submit a Certificate from their Chartered Accountants regarding their financial capability.
- xii. The Auditor/ Firm/ Company/LLP or its group company / subsidiary company / holding company /affiliate /associate company / partner should have never been black listed and/or banned and /or barred and / or disqualified and or prohibited by SEBI and /or RBI and /or NCLT and/ or NCLAT and / or any court of law and / or quasi-judicial authority / and or any other statutory and/ or regulatory authority, in undertaking any work directly or indirectly which is required to perform as stated in this RFP and/ or issuance of any

certificate of audit directly or indirectly with respect to the work sated herein the RFP.

- xiii. The bidder should submit a certificate in support of ISO 9001 in support of certification of services, and to be ensured that the certificate will remain valid for entire contract duration.
- xiv. The bidder must have arrangements/back to back tie-ups with OEM to undertake all software upgrades / modifications necessary to conform to any changes or modifications required by the Bank and in compliance of RBI/ regulatory compliance(in time bound manner), from time to time, during the contract period .
- xv. The Proposed Security solutions is in adherence to the guidelines provided in the RBI cyber security circular no RBI/2015-16/418 dated 2nd June 2016 and its subsequent amendments (in present and in future)
- xvi. A summary of deployment/ implementation establishing the bidder's experience and OEM/product capability must be enclosed with the Technical Bid, giving the following details:
- Name of the Client.
 - Number of branches.
 - Nature of the Project.
 - Scope of the Project.
 - Project Deliverables.
 - Hardware and Software environments of the Project.
 - Architecture of the solution implemented, including network architecture.
 - Date of award of Contract.
 - Date of commencement of the Project.
 - Date of successful commissioning of the Project (Pilot / Live).
 - Whether the Project has been vetted / audited by any independent Agency/ Institutional Consultants of Repute, and if so, outcome thereof.
 - Name of the person who can be referred to from Clients' side, with Name, Designation, Postal Address, Contact Phone and Fax numbers, E-Mail IDs, etc. (Enclose copies of purchase orders).

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

- xvii. For “Mobile Device Management “, the solution must be in Leaders Quadrant of Gartner Report. The necessary latest Gartner Report should be attached along with Technical bid.
- xviii. For “Secure web gateway/web proxy solution “, the solution must be in Leaders or Challengers Quadrant of Gartner Report. The necessary latest Gartner Report should be attached along with Technical bid.

(Above details are MANDATORY and are to be included in technical bid. Without the above details, the Bid is liable to be rejected.)

3.5 Cost of Bidding

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

B. The Bidding Documents

3.6 Content of Bidding Documents

3.6.1 The products required, Bidding procedures, and contract terms are prescribed in the Bidding Documents. The Bidding Documents include:

- (a) PART 1 - Invitation to Bid (ITB)
- (b) PART 2 - Disclaimer
- (c) PART 3 - Instruction for Bidders (IFB)
- (d) PART 4 - Terms and Conditions of Contract (TCC)
- (e) PART 5 - Functional Specifications (FS)
- (f) PART 6 - Bid Forms, Price Schedules and other formats (BF)
- (g) PART 7 - Other Terms and Conditions. (OTC)

3.6.1 The bidder is expected to examine all instructions, forms, terms and specifications in the Bidding Document. Failure to furnish all information required by the Bidding Document or to submit a Bid not substantially responsive to the Bidding Document in every respect will be at the Bidder’s risk and may result in the rejection of the Bid.

3.7 Clarification of Bidding Documents

- 3.7.1 Bidder requiring any clarification of the Bidding Document may notify the Bank in writing at the address or by e-mail indicated in Invitation to Bid on or before 11-05-2020 up to 03:00 pm.
- 3.7.2 A **pre-bid meeting** is scheduled on 13-05-2020 at 03:00 pm. Relaxation in any of terms contained in the Bid, in general, will not be permitted, but if granted, the same will be put up on Bank's Website.

3.8 Amendment of Bidding Documents

- 3.8.1 At any time prior to the deadline for submission of Bids, the Bank, for any reason, whether, at its own initiative or in response to a clarification requested by a prospective Bidder, may modify the Bidding Document, by amendment.
- 3.8.2 Notification of amendments will be put up on the Bank's Website and will be binding on all Bidders.
- 3.8.3 In order to allow prospective Bidders reasonable time in which to take the amendment into account in preparing their Bids, the Bank, at its discretion, may extend the deadline for a reasonable period as decided by the Bank for the submission of Bids.

C. PREPARATION OF BID

3.9 Language of Bid

The Bid prepared by the Bidder, as well as all correspondence and documents relating to the Bid exchanged by the Bidder and the Bank and supporting documents and printed literature shall be written in English.

3.10 Format and Signing of Bid

- 3.10.1 Each bid shall be in two parts:-

Part I- Technical Proposal.

Part II- Price Proposal.

The two parts should be in two separate covers, each super-scribed with the name of the Project as well as “Technical Proposal” and “Price Proposal” as the case may be.

3.10.2 The Bid shall be typed or written in indelible ink and shall be signed by the Bidder or a person or persons duly authorized to bind the Bidder to the Contract. The person or persons signing the Bids shall initial all pages of the Bids, except for un-amended printed literature.

3.10.3 Any inter-lineation, erasures or overwriting shall be valid **only** if they are initiated by the person signing the Bids. The Bank reserves the right to reject bids not confirming to above.

3.11 Documents Comprising the Bid

3.11.1 Documents comprising the Technical Bid Envelope, should contain the following:

- a. Organizational Profile as per format 6.10.
- b. Conformity to Eligibility Criteria in accordance with clause 3.4 as per format 6.16.
- c. Bid Form as per Format 6.1.1 and duly signed by the Bidder.
- d. Documentary evidence establishing that the products, systems and ancillary services to be supplied by the Bidder are eligible products and services and conform to Part 5 of the Bidding Document.
- e. Non-Disclosure Agreement as per Format 6.2.
- f. Bid Security deposit of Rs.50,00,000/- (Rupees Fifty lakhs only) as specified in Clause 3.17.
- g. Manufacturer’s / Producers’ authorization form as per format 6.8 wherever applicable.
- h. Service Support Details form as per Format 6.11.
- i. Bidders undertaking for support services as per format 6.14 that adequate specialized expertise are available to ensure the fault free operation of the proposed solution and maintenance during the support period.

- j. A Complete Bill of Material with quantity, module name, version etc. as per format 6.13. Please note that no price should be mentioned in this Format.
- k. A full description of the Technical Solution and its compliance, which must provide an acceptable solution as described in PART 5: Functional Specifications in the form of literature, drawing and data.
- l. Details of Projects Handled / Referral Letters as required to support eligibility criteria and scope of work.
- m. Additionally a **Masked price bid should be kept with the Technical bid (i.e. in same format of Format 6.3 (but without any commercials) with detailed Bill of Material matching with Un-Masked Price Bid deliverables**, as “Bill of Materials” as per format 6.13, to be kept in another separate closed / sealed cover. **Please note that no price should be mentioned in this format.**
- n. While submitting the Bid, forms like those of Bid Security, MAF as mentioned above, etc. should form the main section and should be submitted in one lot, separate from the section containing literature on the proposed solution and annual accounts.

3.11.2 Documents comprising Price Bid Envelope, should be :

- a) A Full Price Schedule of the Solution indicating all the components of the solution and services (Format 6.3 Part I, Part II and Part III) and format 6.13 **with the prices**, in one separate closed sealed cover.
- b) The Bid as per Format 6.1.2 as furnished in the Bidding Documents duly signed by the Bidder and completed.
- c) Price bids containing any deviations or similar clauses will be summarily rejected.

3.12 Bid Submission

The Bidder shall complete both the Envelopes of the Bid Forms furnished in the Bidding Document separately. Bids are liable to be rejected if only one (i.e. Technical Bid or Price Bid) is received.

3.13 Bid Prices

3.13.1 The prices indicated in the Price Schedule shall be entered in the following manner:

- a) The total price quoted must be **inclusive** of cost of providing product, licensing, hardware, services for installation, testing and commissioning of the Solution and support, all applicable taxes, duties, levies, charges etc., as also cost of incidental services **such as** transportation, insurance, training etc., but **exclusive** of Goods and Services Tax(GST) as applicable
- b) Prices quoted as above shall be valid for contract period from last date for submission of the tender. **The bidder cannot quote for the project in part.**

3.13.2 Prices quoted by the Bidder shall be fixed during the Bidder's performance of the Contract and shall not be subject to variation on any account, including exchange rate fluctuations, changes in taxes, duties, levies, charges etc. during period of contract. A Bid submitted with an adjustable price quotation will be treated as non-responsive and will be rejected.

3.13.3 However, during the contract period, if the market price of services have been on the lower side, the Bank will request the vendor to revise the rates with mutual consent.

3.14 Bid Currencies

Bids are to be quoted in **Indian Rupees** only.

3.15 Documents Establishing Bidder's Eligibility and Qualifications

3.15.1 The bidder shall furnish, as part of its Bid, documents establishing the bidder's eligibility to Bid and its qualifications to perform the Contract, if its Bid is accepted.

3.15.2 The documentary evidence of the bidder's qualifications to perform the Contract if its Bid is accepted, shall establish to the Bank's satisfaction:

- a) that, in the case of a bidder offering to supply products and/or systems under the Contract which the bidder did not produce, the bidder has been duly authorized as per authorization format 6.8 given in the Bid, by the products' producer to supply the products and/or systems in India;
- b) that the Bidder has the technical and production capability necessary to perform the Contract as per format 6.10 (Organization Profile);
- c) ***that adequate, specialized related software expertise is already***

available, to ensure that the support services are responsive, and the bidder will assume total responsibility for the fault-free operation of the solution proposed and maintenance till the end of support period of 5 years.

3.16 Documents Establishing Eligibility of Products and Conformity to Bid Documents

3.16.1 The Bidder shall furnish, as part of its Bid, documents establishing the eligibility and conformity to the bidding documents of all products and / or system and/or services, which the bidder proposes to supply under the Contract.

3.17 Bid Security

3.17.1 The Bidder shall furnish, as part of its Bid, a Bid Security as specified in Clause 3.11.1 (f).

3.17.2 The Bid security is required to protect the Bank against the risk of bidder's conduct, which would warrant the security's forfeiture.

3.17.3 The Bid security shall be denominated in Indian Rupees and shall be in following forms:

a bank guarantee issued by a scheduled commercial bank/nationalized public sector bank in India (other than Bank of India), acceptable to the Bank, in the form as per format 6.4 provided in the Bid, valid for one year with three months claim period;

3.17.4 Any Bid not secured, as above, will be rejected by the Bank, and treated as non-responsive.

3.17.5 Bank will follow the guidelines issued by Govt. of India for MSME units registered with NSIC under single point registration scheme. In case of bidders registered with NSIC, they are eligible for waiver of EMD. However, they need to provide valid NSIC Certificate clearly mentioning that they are registered with NSIC under single point registration scheme. No interest will be payable on the Bid Security amount.

3.17.6 Unsuccessful bidders' Bid security will be discharged or returned as promptly as possible but not later than Ninety (90) days after awarding the contract to successful bidder (i.e. not later than prescribed by the Bank).

3.17.7 The successful bidder's Bid security will be discharged upon the bidder signing the Contract and furnishing the performance security as per format 6.6.

3.17.8 The Bid security may be forfeited:

- a) if a bidder withdraws its Bid during the period of Bid validity specified by the bidder on the Bid Form; or
- b) if a bidder makes any statement or encloses any form which turns out to be false / incorrect at any time prior to signing of Contract; or
- c) in the case of a successful bidder, if the bidder fails;
 - (i) to sign the Contract;

OR

- (ii) to furnish Performance Security, as mentioned in Clause 4.4 herein.

3.18 Period of Validity of Bids

3.18.1 Bids shall remain valid for a period one year, from the last date of submission of the Bid. A Bid valid for a shorter period shall be rejected by the Bank as non-responsive.

3.18.2 In exceptional circumstances, the Bank may solicit the bidders' consent to an extension of the period of validity. The request and the responses thereto, shall be made in writing. The Bid security provided shall also be suitably extended. A bidder may refuse the request without forfeiting its Bid security.

D. Submission of Bids

3.19 Sealing and Marking of Bids

3.19.1 The Bidders shall seal the envelopes containing "Technical Bid" and "Price Bid" separately and the two envelopes shall be **enclosed and sealed in an outer envelope**. The Bidder should additionally submit soft copies of the Technical Specification in the form of CD.

3.19.2 The inner and outer envelopes shall:

- a) be addressed to the Bank at the address given; and

- b) bear the Project Name **RFP for Supply, Implementation and Maintenance of IT Security Solutions** at Bank of India.”, and a statement: **“DO NOT OPEN BEFORE 29.05.2020”**.
- c) All envelopes should indicate on the cover the name and address of the bidder.

3.19.3 If the outer envelope is not sealed and marked, the Bank will assume no responsibility for the Bid’s misplacement or premature opening.

3.20 Deadline for Submission of Bids

3.20.1 Bids must be received by the Bank at the address specified, no later than the date and time specified in the Invitation to Bid.

3.20.2 The Bank may, at its discretion, extend this deadline for the submission of Bids by amending the Bid Documents, in which case, all rights and obligations of the Bank and bidders, previously subject to the deadline, will thereafter be subject to the deadline as extended.

3.21 Late Bids

3.21.1 Any Bid received by the Bank after the deadline for submission of Bids prescribed, will be rejected and returned unopened to the Bidder.

3.22 Modification and Withdrawal of Bids

3.22.1 The Bidder may modify or withdraw its Bid after the Bid’s submission, provided that written notice of the modification, including substitution or withdrawal of the Bids, is received by the Bank, prior to the deadline prescribed for submission of Bids.

3.22.2 The Bidder’s modification or withdrawal notice shall be prepared, sealed, marked and dispatched. A withdrawal notice may also be sent by fax, but followed by a signed confirmation copy, postmarked not later than the deadline for submission of Bids.

3.22.3 No Bid may be modified after the deadline for submission of Bids.

3.22.4 No Bid may be withdrawn in the interval between the deadline for submission of Bids and the expiration of the period of Bid validity specified by the bidder on the Bid Form. Withdrawal of a Bid during this interval may result in the bidder’s forfeiture

of its Bid security.

E. Bid Opening and Evaluation

3.23 Opening of Bids by the Bank

3.23.1 The bidders' names, Bid modifications or withdrawals and the presence or absence of requisite Bid Security and such other details as the Bank, at its discretion, may consider appropriate, will be announced at the Bid opening. No bid shall be rejected at bid opening, except for late bids, which shall be returned unopened to the Bidder.

3.23.2 Bids (and modifications sent) that are not opened at Bid Opening shall not be considered further for evaluation, irrespective of the circumstances. Withdrawn bids will be returned unopened to the Bidders.

3.24 Clarification of Bids

3.24.1 During evaluation of the Bids, the Bank, at its discretion, may ask the bidder for clarification of its Bid. The request for clarification and the response shall be in writing, and no change in the prices or substance of the Bid shall be sought, offered, or permitted.

3.25 Preliminary Examination

3.25.1 The Bank will examine the Bids to determine whether they are complete, required formats have been furnished, the documents have been properly signed, and the Bids are generally in order.

3.25.2 The Bank may, at its discretion, waive any minor infirmity, non-conformity, or irregularity in a Bid, which does not constitute a material deviation.

3.25.3 The Bank will first examine whether the Bid and the bidder is eligible in terms of eligibility criteria.

3.25.4 Prior to the detailed evaluation, the Bank will determine the substantial responsiveness of each Bid to the Bidding Document. For purposes of these Clauses, a substantially responsive Bid is one, which conforms to all the terms and conditions of the Bidding Document, without material deviations. Deviations from, or objections or reservations to critical provisions, **such as** those concerning Bid Security, Applicable Law, Performance Security, Qualification Criteria, Insurance, AMC and Force Majeure will be deemed to be a material deviation. The Bank's determination of a Bid's responsiveness is to be based on the contents of the Bid

itself, without recourse to extrinsic evidence. The Bank reserves the right to evaluate the bids on technical and functional parameters, including possible visit to inspect live site/s of the Vendor and witness demos of the system and verify functionalities, response times, etc.

3.25.5 If a Bid is not substantially responsive, it will be rejected by the Bank and may not subsequently be made responsive by the bidder by correction of the non-conformity. The technical evaluation will take into account the capability of the bidder to implement the proposed solution.

3.25.6 Only those bidders whose Technical bids have been found substantially responsive would be intimated by the Bank about their responsiveness and about the revised / updated Technical & Functional Specification (if any) arising out of normalization (if any). In case of normalization and/or revision, they would also be advised to submit fresh "Price Bid" which should either be equal to or less than the Prices quoted in the Original Price Bid. The Original and revised price bids as above would then be opened in the presence of the bidders' representatives on a specified date and time to be intimated to the respective bidders. The lower of the two prices quoted by the bidders shall only be reckoned for the purpose of price evaluation.

3.26 Technical Evaluation

3.26.1 Only those bidders and Bids who have been found to be in the conformity of the eligibility terms and conditions during the preliminary evaluation, would be taken up by the Bank for further detailed evaluation. Those Bids, which do not qualify the eligibility criteria and all terms during preliminary examination, will not be taken up for further evaluation.

3.26.2 The Bank may use the services of external consultants for technical evaluation.

3.26.3 The Bank reserves the right to evaluate the bids on technical and functional parameters, including visit to inspect live site/s of the bidder and witness demos of the system and verify functionalities, response times, etc in which all the travelling/lodging etc. expenses will be borne by the Bidder.

3.26.4 The Bank will do the evaluation on the responses provided by the bidder in the Format 6.16.

3.26.5 Bank reserves the right to waive any of the Technical and Functional Specifications during technical evaluation, if in the Bank's opinion it is found to be minor deviation or acceptable deviation.

3.26.6 Bill of Materials (with Masked Price Schedule) submitted along with Technical Bid will be first evaluated and if the Bank, during the evaluation, deems it fit, may request bidder to revise the bill of materials submitted originally in the pricing schedule. If the bidder does not agree to revise the same within 5 days from the date of notification to revise the price bid submitted, it will be considered non-responsive and accordingly rejected.

3.26.7 During evaluation of the Bids, the Bank, at its discretion, may ask the bidder for clarification of its Bid. The request for clarification and the response shall be in writing, and no change in the prices or substance of the Bid shall be sought, offered or permitted.

3.27 Opening of Price Bids / Reverse Auction

3.27.1 Only those bids which are found to be technically responsive will be informed of the date / time / venue of opening of price bids / reverse auction.

3.27.2 The Technical Bids will be evaluated as per eligibility criteria. Thereafter the Bank reserves the right of selection of vendor by opening of Commercial Bids or rates quoted by the vendors in reverse auction (who are found eligible after evaluation of Technical Bids).

Reverse auction with unlimited extensions (default extension period of 10 minutes) will be conducted. The reverse auction shall get closed automatically, when no bid is received in an extension period.

3.27.3 After opening of price bids and declaring the prices, the Bank will evaluate and compare the Price Bids. Alternatively, the Bank may shortlist the vendors, who were found eligible after evaluation of Technical Bids, for participating in the reverse auction after opening the price bids.

3.27.4 Arithmetical errors will be rectified on the following basis. If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail, and the total price shall be corrected. If the Successful Bidder does not accept the correction of the errors, its Bid will be rejected, and its Bid security may be forfeited. If there is a discrepancy between words and figures, the amount in words will prevail.

3.27.5 The Bank's evaluation of a Price Bid will take into account, in addition to the Bid price quoted, one or more of the following factors:

- a) Deviations in payment schedule & Delivery Schedule from that specified;
- b) Deviation in prices quoted;
- c) Other specific criteria indicated in the Bid and/or in the Technical & Functional Specifications & Price schedule.

3.27.6 For factors retained in the Bid, one or more of the following quantification methods will be applied:

(a) Payment schedule.

TCC Clause 4.12 and 4.18 stipulates the payment schedule offered by the Bank.

(b) Delivery Schedule:

b.1 .1 Delivery and Installation Schedule:

- i. All products and/or Systems and/or Services covered under this bid shall be supplied, installed and commissioned by the bidder within the **20 weeks'** time in which DC and DR Setup are to be delivered within **8 weeks** & implementations of software solutions/its agents at all end points should be rolled out/ done within **12 weeks** of period after delivery of solution at central locations (DC and DR). The bidder can start implementation after delivery immediately. No credit will be given to early deliveries. For delayed deliveries & installation, liquidated damages shall be applicable as mentioned in related clause of the RFP.
- ii. The above activity is time bound and proper co-ordination from successful bidder with OEM for end-to-end delivery/ installation/ integration is expected for the success of the project.
- iii. The purchase order will be deemed accepted from 7th day of purchase order date, in case bidder does not convey formal acceptance to Bank.
- iv. For additional procurement of deliverables (i.e. solution for RRBs, additional licenses) during the contract period, same delivery and installation schedule will be applicable, as in present deliverables.

- v. The above delivery schedule shall be applicable for each solution, hence bidder should plan parallel deployment to achieve implementation of all solution in aforementioned duration.

b.2 Delivery Schedule for Facility Management Services:

- i. The bidder shall deploy all the facility management services/resources within **12 weeks** from the date of purchase Order. Bidder shall ensure complete availability in line to roster/requirement mentioned in the scope of Facility Management Support. The start date of FMS shall be start date of contract or date of deployment of resources whichever later. The resources shall be deployed well within time.
- ii. As FMS is integrated part for ensuring smooth support/services for running of Solution, the availability of FMS as per defined skills/educational qualifications in the RFP shall be mandatory with in stipulated timelines.
- iii. The Roll out team / Implementation team shall be different from regular resources. No credit will be given to early deliveries. For non-availability / part –availability of resources, the related deduction will be done.

(c) Quotation of Prices for all Items.

The Bidder should quote for complete consignment of items proposed / listed in this Bid. In case, prices are not quoted by any bidder for any specific item / product / service for the purpose of evaluation, the highest of the prices quoted by other bidders, participating in the bidding process, will be reckoned as the notional price for that product / service, for that bidder. However, if selected, at the time of award of Contract, the lowest of the price(s) quoted by other bidders (whose Price Bids are also opened) for that product / service will be reckoned. This shall be binding on all the bidders. However, the Bank reserves the right to reject all such incomplete bids.

3.28 Contacting the Bank

3.28.1 No Bidder shall contact the Bank on any matter relating to its Bid, from the time of opening of Bid, to the time the Contract is awarded.

3.28.2 Any effort by a bidder to influence the Bank in its decisions on Bid evaluation, Bid comparison or contract award, may result in the rejection of the bidder's Bid.

F. Award of Contract

3.29 Post-qualification

3.29.1 All the bids, after their evaluation on the parameters mentioned above, would be arranged in ascending order and the L1 Bidder would be identified as one successful bidders.

3.29.2 If L1 Vendor fails to execute the order, Bank will be free to award the contract to L2 Vendor on the same terms at which the contract was awarded to L1 vendor.

3.30 Bank's Right to Accept Any Bid and To Reject Any or All Bids.

3.30.1 The Bank reserves the right to accept or reject any Bid, and to annul the bidding process and reject all Bids at any time prior to contract award, without thereby incurring any liability to the affected bidder or bidders, or any obligation to inform the affected bidder or bidders of the grounds for the Bank's action.

3.30.2 After identification of L1 Bidder, the Bank will follow the procedure for necessary approvals and thereafter proceed with notification of award to L1.

3.31 Award Criteria

3.31.1 The Bank will award the Contract to the successful bidder who has been determined to qualify to perform the Contract satisfactorily, and whose Bid has been determined to be responsive, and is the highest complying and evaluated Bid.

3.32 Notification of Award

3.32.1 Prior to expiration of the period of Bid validity, the Bank will notify the successful bidder in writing or by fax, that its Bid has been accepted.

3.32.2 The notification of award will constitute the formation of the Contract.

3.32.3 Upon the successful bidder's furnishing of Performance Security, the Bank will promptly notify each unsuccessful bidder and will discharge its Bid security.

3.32.4 Failure of the successful bidder to comply with the requirement, shall constitute sufficient grounds for the annulment of the award and forfeiture of the Bid Security, in which event the Bank may award the contract to the next highest evaluated Bidder, i.e. L2 or so on, or call for new Bids.

3.33 Signing of Contract

3.33.1 At the time when the Bank notifies the successful bidder that it's Bid has been accepted, the Bank will send the bidder the Contract Form as per format 6.5, incorporating all agreements between the parties. The bank reserves the right to incorporate additional clauses as per legal and regulatory requirements of the Bank.

3.33.2 Within the period prescribed, the successful Bidder shall sign and date the Contract and return it to the Bank. The necessary charges/ stamping shall be borne by selected bidder. The contract shall be submitted in two true copies.

3.34 Performance Security

The bidder shall furnish a performance Security/ Performance Bank Guarantee as mentioned in clause 4.4.

3.35 Contract Start date and Duration

The Contract Term / Project period to be considered as 5 years from the starting of the contract i.e. **date of Implementation of central setup at DC and DR (in high availability and redundancy) and installation/availability of solution at minimum 10 % of ordered endpoint or minimum 1000 nodes/ end points of the Bank/Branches whichever is higher for each solution with all enabled features as per RFP.** The setup should have augmentation capacity to cater the future requirements.

Note: Notwithstanding anything said above, the Bank reserves the right to reject / award the contract to any vendor or cancel the entire process without assigning reasons thereto.

PART 4: TERMS AND CONDITIONS OF CONTRACT (TCC)

TABLE OF CLAUSES

Clause No.	Topic	Clause No.	Topic
4.1	Definitions	4.21	Termination for Insolvency
4.2	Use of Contract Documents and Information	4.22	Termination for Convenience
4.3	Patent Rights/Intellectual Property Rights	4.23	Resolution of Disputes
4.4	Performance Security/Performance Bank Guarantee	4.24	Governing Language
4.5	Inspection and Quality Control Tests	4.25	Applicable Law
4.6	System & Other Software	4.26	Addresses for Notices
4.7	Acceptance Tests and Certificates	4.27	Taxes and Duties
4.8	Manuals / Documents	4.28	Supplier Integrity
4.9	Incidental Services	4.29	Supplier's obligations
4.10	Annual Maintenance Contract / Support	4.30	Site Preparation and Installation
4.11	Training	4.31	Commissioning of the Solution
4.12	Payment	4.32	Technical Documentation
4.13	Prices	4.33	Right to use defective product
4.14	Change Orders	4.34	Repeat Orders
4.15	Contract Amendments	4.35	Limitation of Liability
4.16	Assignments	4.36	Indemnity
4.17	Delay in Supplier's Performance	4.37	Confidentiality
4.18	SLA, Uptime & Liquidated Damages	4.38	Weekly Reporting and Reviewing
4.19	Termination for Default	4.39	Independent External Monitors (IEM)
4.20	Force Majeure	4.40	Integrity Pact

PART 4: TERMS AND CONDITIONS OF CONTRACT (TCC)

4.1. Definitions

In this Contract, the following terms shall be interpreted as indicated:

- 4.1.1. "Solution" means providing comprehensive **Supply, Implementation and Maintenance of IT Security Solutions** at the Bank's head office, as indicated in Part 5 of this document.
- 4.1.2 "Supplier" is the successful bidder, who has been determined to qualify to perform the Contract satisfactorily, and whose Bid has been determined to be substantially responsive, and is the highest evaluated Bid.
- 4.1.3 "The Contract" means the agreement entered into between the Bank and the Supplier, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto, and all documents incorporated by reference therein;
- 4.1.4 "The Contract Price" means the price payable to the Supplier under the Contract for the full and proper performance of its contractual obligations;
- 4.1.5 "The Product" means the Security Solutions, which the Supplier is required to service to the Bank under the Contract;
- 4.1.6 "The Services" means those services ancillary to the supply of the Products, such as, installation, commissioning, customization, provision of technical assistance, training, maintenance and other such obligations of the Supplier covered under the Contract;
- 4.1.7 "TCC" means the Terms and Conditions of Contract contained in this section;
- 4.1.8 "The Project Site" means the any premises of the Bank anywhere in India where Security Solutions at Bank of India.

In case of a difference of opinion on the part of the bidder in comprehending and/or interpreting any clause / provision of the Bid Document after submission of the Bid, the interpretation by the Bank shall be binding and final on the Bidder.

4.2 Use of Contract Documents and Information

- 4.2.1 The Supplier shall not, without the Bank's prior written consent, disclose the Contract, or any provision thereof, or any specification, plan, sample or information furnished by or on behalf of the Bank in connection therewith, to any person other than a person employed by the Supplier in the performance of the Contract. Disclosure to any such employed person shall be made in confidence and shall extend only as far as may be necessary for purposes of such performance.
- 4.2.2 The Supplier shall not make use of any document or information enumerated in this Bidding Document except for purposes of performing the Contract without the Bank's prior written consent.
- 4.2.3 Any document, other than the Contract itself, enumerated in this Bidding Document shall remain the property of the Bank and shall be returned (all copies) to the Bank on completion of the Supplier's performance under the Contract, if so required by the Bank.
- 4.2.4 The Bidder shall sign a Non-disclosure Agreement as per Format 6.2.

4.3 Patent Rights/Intellectual Property rights

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

4.4 Performance Security/ Performance Bank Guarantee

- 4.4.1 The Selected bidder shall furnish an unconditional and irrevocable Bank Guarantee for 10% of the total value of contract, in favour of the Bank, from a scheduled Commercial Bank, other than Bank of India, towards **performance of the contract** in accordance with the specification and conditions of the bid document and agreed upon on final bid evaluation. The above guarantee shall be submitted by the bidder within 30 days from the Purchase Order date or at the earliest after award of contract within a month time. The Contract Performance guarantee shall be kept

valid up to end of the contract period i.e. for five years from the start date of the contract, with **continuous period, without any break period**. The guarantee shall contain a claim period of three months from the last date of validity.

- 4.4.2 The proceeds of the Performance Security shall be payable to the Bank as compensation for any loss resulting from the Service Integrator's failure to complete its obligations under the Contract.
- 4.4.3 The Performance Security shall be denominated in Indian Rupees and shall be by way of Bank Guarantee issued by a Public Sector Bank in India (Other than Bank of India), acceptable to the Bank in the format 6.6 provided in the Bid. Bank has full right to add further details in the above mentioned performance security format for protecting the bank's interest.
- 4.4.4 The Performance Security will be discharged by the Bank and returned to the Service Integrator within 90 days after claim period, following the date of completion of the Service Integrator's performance and other obligations under the Contract.
- 4.4.5 In the event of any contract amendment, the Service Integrator shall furnish the amendment to the Performance security within 30 days after receipt of such amendment, rendering the same valid for the duration of the Contract. In the event of any correction of defects or replacement of defective system during the maintenance period the performance guarantee for a proportionate value shall be extended for affected duration.
- 4.4.6 The Bank reserves the right to recover any dues payable by the selected bidder from any amount outstanding to the credit of the selected bidder, including the pending bills and/or invoking Performance Guarantee, if any, under this contract.

4.5 Inspection and Quality Control Tests

- 4.5.1 The Bank reserves the right to carry out pre-shipment inspection by a team of Bank Officials, of any of the existing live installations of the Supplier, referred to in the Technical Bid or demand a demonstration of the solution proposed on a representative model in the bidder's office.
- 4.5.2 The Bank's right to inspect, test and, where necessary, reject the Products after the Products' arrival at the destination, shall in no way be limited or waived by reason of the Products having previously been inspected, tested, and passed by the Bank or its representative, prior to the Products' shipment from the place of origin.

4.5.3 Nothing stated hereinabove shall in any way release the Supplier from any obligations under this Contract.

4.5.4 Project management, Reporting, Reviewing & Timelines

4.5.4.1 Project Planning, Monitoring and Control:

i. The Bidder shall develop a Project Management Plan. The plan shall also detail all milestones and indicate when the required deliverable will be available to Bank

ii. The Project Management Plan shall address at a minimum, the following Service(s) processes:

A. Document Control

B. Design/ Implementation Methodology

C. Change Management

D. Inspection and Testing

iv. The progress of the implementation shall be monitored on regular basis and the deviations, exceptions shall be analysed and corrective actions to be recommended / suggested

v. The Deliverables shall be as per Project Management Plan and Scope of the RFP and

vi. Progress Reports shall be submitted to Bank at key milestones

4.5.4.2 Bidder should submit a weekly report on the development of the project along with reasons of delay, if any, till date of full commissioning.

4.5.4.3 Periodical meetings (fortnightly and monthly) will be held at Bank's premises between the Bidder and the Bank, to review the progress and the Bidder will be required to attend all such meetings and share the minutes of meetings and subsequent progress of highlighted concerns and points of the Bank

4.5.5 Project timelines

Bidders are requested to add any number of phases in the timeline and present it during the presentation, if required. Also timelines can be shown for group of

products but the project timeline should cover all the solutions which are being procured as part of this RFP.

4.6 System & Other Software:

For the System & Other Software, the following will apply:

The Supplier shall provide complete and legal documentation of subsystems, **licensed system product and software, licensed utility software and other licensed software**. The Supplier shall also provide licensed software for all software products, whether developed by it or acquired from others. The Supplier shall also indemnify the Bank against any levies/penalties on account of any default in this regard.

4.7 Acceptance Tests and Certificates:

- 4.7.1 The Acceptance criteria for Solutions for Branches are subject to Installation reports and User Acceptance Test (UAT) Certificate signed by the Bank/ Branch officials for installed solution after its successful commissioning and with satisfactory access of all the applications required.
- 4.7.2 The installation reports/ User Acceptance Test (UAT) Certificate should be in format duly vetted and checked by the bank officials as per requirements. Installation reports and User Acceptance Test (UAT) Certificate shall be duly signed by Bank officials and bidder's engineer for installed endpoints with satisfactory access of all the applications required.
- 4.7.3 The Acceptance Test Procedures (ATP) to demonstrate the feature, quality, and capabilities of all equipment supplied and installed by the bidder as per bank requirements, such as solution, Software (with required licenses) and its integration with other applicable solutions etc. The ATP shall be finalized on basis of scope defined in this RFP with the selected bidder. Bidder shall plan in advance the locations for which the pilot ATP is to be conducted with bank designated official. Bidder shall demonstrate all the features to Bank Officials for signing the ATP. Bidder and Bank officials shall sign ATP document after checking all applications accessibility. Pending completion of acceptance tests, the bank reserves the right to use the system and such usage shall not be deemed as acceptance of the system by the selected bidder. Unsatisfactory performance in interconnectivity or integration or migration may result in the Bank's rejection of part or all of the system.

4.7.4 On successful completion of the acceptance tests, receipt of deliverables, etc., and after the solution runs successfully after going live and Bank is satisfied with the working of the solution/system, the acceptance certificate, signed by the Supplier and the representative of the Bank will be issued. The date on which such certificate is signed shall be deemed to be the date of successful commissioning of the system/solution proposed.

The system will be considered accepted (supplied, installed and operationalized) only after working of full-fledged, equivalent setup in DC and DR in high level redundancy which is duly signed/certified by the Bank as per the scope mentioned herein this RFP.

Some of features required to be completed are enumerated below:

- i. The delivered software should correspond to what is stated in the purchase order without deviation, except where mutually agreed upon.
- ii. The product/ software is fully installed and integrated with existing environment.
- iii. Certification from product / software OEM's for installation of solution with best practice.
- iv. The User acceptance certificate shall be drafted by the bidder and approved by the Bank. The format shall be part of project plan document.

4.7.5 On successful completion of the acceptance tests, receipt of deliverables, etc., and after the solution runs successfully after going live and Bank is satisfied with the working of the solution/system, the acceptance certificate, signed by the Supplier and the representative of the Bank will be issued. The date on which such certificate is signed shall be deemed to be the date of successful commissioning of the system/solution proposed.

If, any components and/or software fails to pass the acceptance test, bidder shall be given maximum 30 days to rectify the defects and pass the acceptance test; failing which Bank reserves the right to get the respective component (Hardware/Software) replaced (replacement to be completed within max 21 days) by the bidder at no additional cost to Bank. If replacement not done by bidder, Bank reserves the right to cancel the order and recall all the payments made by Bank or invoke performance bank guarantee. No request for extension of period for rectification of defects will be considered from the bidders. Bank reserves rights in this matter.

4.8 Manuals / Documents

- i. Before the products/system is/are taken over by the Bank, the Supplier shall supply technical/systems manuals for all software supplied and for all interfaces etc. Operation and maintenance manuals for all systems and applications systems, covering at least the operations needed to start, run the system during operational day, close, restore, archive, recover from failures, and transfer to fallback system/site including business continuity plan to be provided by the vendor. User manuals for all locations DC, DR, service branch, Branches, for all modules are to be provided for by the vendor. The manuals shall be in English.
- ii. Unless and otherwise agreed, the products and equipment shall not be considered to be completed for the purpose of taking over, until such manuals have been supplied to the Bank.
- iii. The Supplier shall provide one set of Design Manual, System Manual, User Manual and Security Manual for the Application Software. The Supplier shall also provide one Soft copy of each of the Manuals. Soft and Hard copy User manuals shall be provided, commensurate with number of installations of Products in the Bank.
- iv. Documentation should be comprehensive & include:
 - Product Literature.
 - Operating manuals.
 - General Specifications.
 - Operator Reference manuals for each operator task.
 - Messages manuals.
 - Documentation on troubleshooting.
- v. Delivery of the products/software shall be made by the Supplier in accordance with the system approved/ordered. The details of documents to be furnished by the Supplier are specified hereunder:
 - i. 3 copies of Supplier's invoice showing contract number, products description, quantity, unit price and total amount;
 - ii. Delivery note or acknowledgement of receipt of products from the Consignee or in case of products from abroad, original and two copies of the negotiable, clean Airway Bill;

The above documents shall be received by the Bank before arrival of products (except where it is handed over to the Consignee with all documents) and, if not received, the Supplier will be responsible for any consequent expenses.

4.9 Incidental Services

4.9.1 The incidental services to be provided are as under:

- (a) Furnishing manuals for each appropriate unit of the supplied Products, as mentioned under Clauses 4.8 and other relevant clauses of TCC;
- (b) Maintenance and software updates of the supplied Products, technical support thereof for a period as specified in the SLA/Uptime Clause, from date of go live.

4.10 Annual Maintenance Contract/Support

- 4.10.1 The Supplier warrants that the products supplied under the Contract are of the most recent version and that they incorporate all recent improvements in design and / or features. The Supplier further warrants that all the Products supplied under this Contract shall have no defect, arising from design or from any act of omission of the Supplier that may develop under normal use of the supplied products in the conditions prevailing in India. Professionally qualified personnel, who have expertise in system software supplied by the vendor, will provide these services. The bidder shall follow the scope as mentioned in clause 3.3.9.
- 4.10.2 The Supplier shall comply with the performance guarantees specified under the Contract. If, for reasons attributable to the Supplier, these guarantees are not attained in whole or in part, the Supplier shall make such changes, modifications and / or additions to the Products or any part thereof as may be necessary in order to attain the contractual guarantees specified in the Contract at its own cost and expense and to carry out further performance tests.
- 4.10.3 The Bank shall promptly notify the Supplier in writing of any claims arising under this Annual Maintenance Contract.
- 4.10.4 Upon receipt of such notice, the Supplier shall with all reasonable speed, repair or replace the defective products or part thereof without cost to the Bank.
- 4.10.5 If the Supplier, having been notified, fails to remedy the defect(s) within the period specified, the Bank may proceed to take such remedial action as may be necessary, at the Supplier's risk and expense and without prejudice to any other rights, which the Bank may have against the supplier under the Contract.

- 4.10.6 During Support Period, Supplier guarantees an Uptime of 99.90 % on monthly basis for the entire/core solution proposed. Please refer to SLA/Uptime Clause for details of uptime required by the Bank.
- 4.10.7 AMC for system hardware and Software / off-the-shelf Software will be provided to the Bank as per the general conditions of sale of such software.
- 4.10.8 The maximum response time for a maintenance complaint from the site of installation (i.e. time required for Supplier's maintenance engineers to report to the installations after a request call / fax /e-mail is made or letter is written) shall not exceed 2 (two) hours.
- 4.10.9 The Supplier shall ensure that faults and failures intimated by Bank as above are set right within 4 hours of being informed of the same.
- 4.10.10 The bidder shall ensure re-deployment of Solution at central or remote sites or at endpoints as part of maintenance only. There is no additional charges shall be payable for re-designing / re-deployment of solution at any or all endpoints including DC and DR sites of the Bank. All activities pertaining to continuity of the solution shall be ensured by the bidder as part of AMC without any extra cost to the Bank
- 4.10.11 The Bidder should provide and implement upgrades of the solution during the contract period free of cost.
- 4.10.12 The Bidder should provide changes and upgrades with regard to changes in statutory requirements at the earliest and free of cost during the contract period.
- 4.10.13 The Bidder should provide and implement functionality changes as required by the end user during the contract period.
- 4.10.14 The Bidder should be able to comply with the service Level requirements.
- 4.10.15 The detailed scope is mentioned in clause 3.

4.11 Training

For each solution/ module /database/middleware and third party utilities installed, the Supplier is required to train the designated Bank's technical team in all aspects like resource management of hardware and software, storage allocation, backup management, backup reconciliation and end-user personnel to enable them to effectively

operate and perform administration of the total system. The Bank may ask the bidder to conduct the training without any additional cost. The Supplier is also required to conduct mandatory training for customizations / database management for the administrators specified by the Bank without any additional cost. The Bidders shall provide professional training as mentioned in clause 3.3.2 above.

4.12. Payment Schedule

4.12.1 Payment shall be made in Indian Rupees, as given below for delivering, installing, commissioning and monitoring the Solution / deliverables as mentioned in price schedule.

A. Payment of Solution:

- i. **Payment of Solution Cost/ Implementation Cost - 100%** payment of Solution Cost/ Implementation Cost on successful commissioning of the solution at DC and DR site with full high level redundancy at both the sites, and only after deployment of 10% of licenses at end points , and its signoff from Bank team.
- ii. **Payment of License Cost – The payment can be made in minimum multiple/ lot of 10% of ordered licenses quantity post deployment at end points and signoff from Bank team.**

(Note –Payment of additional license cost (if procured), will be paid in in minimum multiple/lot of 10% of quantity, post deployment at end points and signoff from Bank team.

- iii. The payment frequency shall be quarterly in arrear hence bidder should submit invoices quarterly for payment of delivered services to the Bank.
- iv. The payment shall be made after deducting applicable liquidated damages/penalty.

B. Payment of AMC/ATS

- i. Post warranty, the AMC/ATS charges shall be processed by the bank **quarterly** in arrear within forty five (45) days from the date submission of invoice with adequate and correct supporting documents and after deducting the applicable penalty.

- ii. The payment of services and maintenance will be subjected to satisfactory services rendered and preventive maintenance carried out as per scheduled frequency. The invoice should be clear and with all supporting documents else the payment processing shall be delayed and bank will not be responsible for any delay in non-payment beyond stipulated time to the bidder due to non-availability of supporting documents. The total support period will be five years.

C. Payment of FMS

- i. The Facility Management charges shall be paid by the bank in equal **Quarterly** instalments within forty five (45) days from the date submission of invoice after completion of quarterly period and after deducting the applicable prorated amount of deficit resources and penalty if any.
- ii. The payment of facility management services will be subjected to satisfactory services rendered from the date of commencement of services and acceptance of the support system at the rates quoted in the price schedule. The FMS will be started from the deployment of resources as per requirement and terms under the RFP. The start date of FMS shall be start date of contract or date of deployment of resources whichever later and delivery of monitoring tool for monitoring of all Security Solutions.

D. Payment against Bank Guarantees:

For all the payments to be made against bank guarantees, the bank guarantee shall be issued by a nationalized / public sector bank in India (other than Bank of India), acceptable to the Bank as per Format 6.6 of this RFP. The payment shall be made after availing the services by the Bank and in arrears only.

4.13 Prices

- 4.13.1 Prices payable to the Supplier as stated in the Contract shall be firm and not subject to adjustment during performance of the Contract, irrespective of reasons whatsoever, including exchange rate fluctuations, changes in taxes, duties, levies, charges, etc.
- 4.13.2 The Bidder will pass on to the Bank, the benefit of discounts, if any, announced in respect of the cost of the items for which orders have been placed during that period.

4.14 Change Orders

4.14.1 The Bank may, at any time, by a written order given to the Supplier, make changes within the general scope of the Contract in any one or more of the following:

- (a) Technical and functional specifications
- (b) Services to be provided by the Supplier.

4.14.2 If any such change causes an increase or decrease in the cost of, or the time required for the Supplier's performance of any provisions under the Contract, an equitable adjustment shall be made in the Contract Price or delivery schedule, or both, and the Contract shall accordingly be amended. Any claims by the Supplier for adjustment under this clause must be asserted within thirty (30) days from the date of Supplier's receipt of Bank's change order.

4.15 Contract Amendments

4.15.1 No variation in or modification of the terms of the Contract shall be made, except by written amendment, signed by the parties.

4.16 Assignment

4.16.1 The Supplier shall not assign, in whole or in part, its obligations to perform under the Contract, except with the Bank's prior written consent.

4.17 Delays in the Supplier's Performance

4.17.1 Delivery of the Products and performance of Services shall be made by the **Supplier** in accordance with the time schedule prescribed by the Bank in Clause.

4.17.2 If at any time during performance of the Contract, the **Supplier** or its subcontractor(s) should encounter conditions impeding timely delivery of the Products and performance of Services, the **Supplier** shall promptly notify the Bank in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the **Supplier's** notice, the Bank shall evaluate the situation and may, at its discretion, extend the **Suppliers'** time for performance, with or without liquidated damages, in which case, the extension shall be ratified by the parties by amendment of the Contract.

4.17.3 Except as provided in the above clause, a delay by the **Supplier** in the performance of its delivery obligations shall render the **Supplier** liable to the

imposition of liquidated damages, unless an extension of time is agreed upon without the application of liquidated damages.

4.18 SLA, Uptime & Liquidation Damages

4.18.1 SLA, Uptime & Penalty

The successful bidder is bound and to comply the Service Levels described below:-

- i. The successful bidder shall have to enter into “Service Levels Agreement” having all terms and conditions of this RFP to maintain uptime and provide the service support and onsite support during the entire contract period.
- ii. Both bidder and OEM will be total responsible for the maintenance, configuration and fault free operations of supplied infrastructure i.e. hardware, software and its maintenance during the warranty and post warranty (AMC/ATS period) period.
- iii. Any technical glitch/ issue in installed infrastructure of the solution (i.e. hardware and software, OS/DB etc)) should be attended on priority and should be covered under warranty/AMC.
- iv. The bidder has to maintain guaranteed minimum uptime of **99.90%** for all systems/ solutions supplied under this RFP to avoid any business disruption due to breakdown of system or degraded performance impacting business or unavailability of data. **The calculation of uptime will be on monthly basis.**
- v. The issue/ break down message may be communicated by Bank team by way over phone / email/ call logging.
- vi. For penalty calculation, the total time elapsed between the intimation of break down message from Bank side to the vendor and receipt of rectification message from bidder to Bank side will be considered.
- vii. During warranty period, the penalty will be deducted in quarterly FMS payment. In case, Bank is unable to adjust penalty in FMS payment, the Bank at its

discretion may invoke the Performance Bank Guarantee (PBG) to deduct the penalty amount.

- viii. Post warranty period, the penalty will be deducted in quarterly FMS/AMC/ATS payment. In case, Bank is unable to adjust penalty in FMS/AMC/ATS payment, the Bank at its discretion may invoke the Performance Bank Guarantee (PBG) to deduct the penalty amount.
- ix. If the support services is not provided on 24*7 basis and/or satisfactory services are not provided, Bank with its discretion may reject the proposal / terminate the contract, without assigning any reason.
- x. The bidder is required to mandatorily conduct quarterly preventive and breakdown maintenance activities to ensure (without any impact on day to day operations) to maintain uptime of 99.90% uptime on monthly basis covering 24*7*365 days.
- xi. Apart from maintaining uptime of 99.90%, for any breakdown / malfunctioning of hardware and its any of the components or accessories or any system software issue etc., the resolution time is mentioned below:-

$$\text{Uptime \%} = \frac{((\text{Number of hours in month} - \text{Number of hours impacted in month}) * 100)}{\text{Total Number of hours in month}}$$

- xii. For calculation of uptime (penalty), planned/ scheduled down time will be exempted. Bank will pay to the bidder after deducting the calculated penalty from the payable amount.
- xiii. If any critical component of the entire configuration setup is out of service , then the bidder & OEM shall either immediately replace the defective unit (with new one) or replace it at its own cost or provide a standby , on immediate basis, not more than 4 hours , The bidder should maintain proper inventory of standby components for early resolution of issues.

- xiv. If the bidder, having been notified, fails to remedy the defect(s) within the 4 hours' time duration from the incident, the Bank may proceed to take such remedial action as may be necessary, at the Supplier's risk and expense and without prejudice to any other rights, which the Bank may have against the supplier under the Contract.
- xv. The bidder should comply the security and audit standards of Bank and various regulatory guidelines. For this, the bidder should apply new patches related to OS/ firmware & BIOS updates etc, without any additional cost to the bank, during the contract period.
- xvi. For all issues, related to installed infrastructure, RCA (Root Cause Analysis) to be provided by the respective OEM within 3 working days. The delay in submission will lead to penalty.

Table1: Service Level Agreement and Penalty for Operations

Service Area	Service Level	Penalty
Availability Management		
Coverage of agents	<p>After completing the delivery timelines of the deployment of agents at end points (which will serve the base for coverage). Weekly penalty on coverage of deployed agents on endpoints for agent based solutions.</p> <p>The deployed agent at end of each month will serve as “Base Count” for evaluating coverage for next month.</p>	<p>If the deployed agent coverage is below 90% of Base Count on weekly basis, a penalty of 5 % of monthly contract value per week of the solution will be levied.</p> <p>If the deployed agent coverage is below 80% of Base Count on weekly basis, a penalty of 10% of monthly contract value per week of the solution will be levied.</p> <p>If the deployed agent coverage is below 70% of Base Count on weekly basis, a penalty of 20 % of monthly contract value per week of the solution will be levied.</p>
Uptime of the solution for High availability setup	Uptime % of application calculated on monthly basis for each solution.	Penalty shall be applicable in % (as mentioned below) of monthly contract value.
	99.90% monthly uptime and above	NA
	Below to 99.89%	1 % deduction of monthly contract value for the solution for every reduction in uptime by 0.01 % in uptime. Uptime shall be calculated monthly
Manpower Management		
Manpower Services	Bidder to provide experienced and certified	<ul style="list-style-type: none"> Penalty of Rs. 2000 per week for absence per week or part

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



Service Area	Service Level	Penalty
	manpower at Bank premises as per RFP. Any gap will attract penalty.	thereof for each L1/L2 resources in addition to deduction of relevant day's resource's unit cost. <ul style="list-style-type: none"> Penalty of Rs. 3000 per week for absence per week or part thereof for L3 resource in addition to deduction of relevant day's resource's unit cost.
	Bidder have to replace the manpower if specially asked by the Bank with in a period of one month. A delay beyond next Month billing cycle will attract the penalty.	<ul style="list-style-type: none"> Penalty of Rs. 300 per day for delay in joining of new resource as replacement for L1/L2 resource. Penalty of Rs. 500 per day for delay in joining of new resource as replacement for L3 resource.
	Centralized Management and Monitoring System	
No Deployment or less than 60% functionality	Shall be available with 99.90 % functionalities	30% of monthly ATS& FMS Cost deduction for the entire solution for every month of its non-availability
Partial Deployment (having between 60- 80% functionality)	Shall be available with 99.90 % functionalities	20% of monthly ATS & FMS Cost deduction for the entire solution for every month of its non-availability
Partial Deployment (having between than 80-95% functionality)	Shall be available with 99.90 % functionalities	10% of monthly ATS & FMS Cost deduction for the entire solution for every month of its non-availability
Partial Deployment (having between than 95-99.90% functionality)	Shall be available with 99.90 % functionalities	5% of monthly ATS & FMS Cost deduction for the entire solution for every month of its non-availability

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



Service Area	Service Level	Penalty
Downtime of Centralized Monitoring Tool	Shall be available with uptime of 99.90 % monthly uptime	1 % deduction of monthly total of ATS and FMS value for the solution for every reduction in uptime by 0.01 % in uptime. Uptime shall be calculated monthly
For “Centralized Monitoring System”, ATS post warranty period (i.e. Year 2 of the contract), will be considered during Warranty Period for calculation of penalty.		
	Security Vulnerability Management	
Version Upgrade Major/ Minor for all Software / Middleware	The Operations Team have to have version upgrades of all underlying software / Middleware as per respective OEM recommendations & Publish the Quarterly version upgrade calendar for the same. Failure to comply with Version upgrade calendar will attract penalties.	For breaches of Version upgrade – <ul style="list-style-type: none"> Penalty of Rs.100 per day for delay in version upgrade of (OS, Server, Solution, protocol etc) per day.
Patching of all Hardware / Software / Middleware	All underlying hardware / software / Middleware to be patched as per respective OEM recommendations. Failure to comply with Patch calendar will attract penalties.	For breaches for patches – <ul style="list-style-type: none"> Penalty of Rs.100 per day for delay in applying of each patch as per security/statuary/ OEM recommendations.
Closure of VA / PT , and SCD Points on all Hardware / Software / Middleware	All identified vulnerabilities over underlying hardware / software / Middleware to be patched as per respective OEM recommendations. Failure to close these calls within timelines will attract penalties based on criticality of calls. <ol style="list-style-type: none"> Critical Category– 7 Days High Category – 15 Days Medium - 30 Days 	For breaches for timelines under Critical & High Category – <ul style="list-style-type: none"> Penalty of Rs.300 per day per vulnerability for delay in mitigation/ fixing vulnerabilities. For breaches for timelines under Medium Category –

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



Service Area	Service Level	Penalty
	4.Low Days - 60	<ul style="list-style-type: none"> Penalty of Rs.200 per day per vulnerability for delay in mitigation/ fixing vulnerabilities. <p>For breaches for timelines under Low Category –</p> <ul style="list-style-type: none"> Penalty of Rs.100 per day per vulnerability for delay in mitigation/ fixing vulnerabilities.
	Knowledge Management	<ul style="list-style-type: none">
OEM Training once in 2 years	Training not conducted by OEM to the bank personnel and on-site bidder resources as per requirements of RFP.	<ul style="list-style-type: none"> The OEM training cost of relevant year would not be paid. Additionally, Rs. 2,000 penalty for each such solution for each defaulted month will be imposed.
OEM Health Check	Health check not conducted by the OEM representative once in a year	<ul style="list-style-type: none"> Penalty of Rs. 2,000 will be charged for each such solution for each defaulted month will be imposed.
Compliance of RBI/ CERT-IN Advisories/ other regulatory advisory	Compliance by end date , as notified in the advisory	<ul style="list-style-type: none"> Compliance by end date – No Penalty
	Penalty by delay by each day	By Delay of each day, 0.5% of Monthly Contract Value, per day

(c) During Warranty period, “Monthly Contract Value” will be as under-

Solution Cost /12 + License Cost/12 + FMS Cost/12 (divided by 12 for getting monthly amount out of yearly amount)

(d) Post Warranty period, “Monthly Contract Value” will be as under-

AMC of Solution Cost/12 + AMC/ATS of License Cost/12 + FMS Cost/12
(divided by 12 for getting monthly amount out of yearly amount)

Penalty Cap on SLA: - 100% * Monthly Contract Value (calculated on Monthly basis).

4.18.2 Liquidation Damages/ Penalty for delay

If the **Supplier** fails to deliver /implement the solution (any or all of the Products) 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 0.5 percent per week or part thereof of total contract price subject to maximum deduction of 10% of the total contract value for the solution or unperformed services for each week or part thereof of delay, until actual delivery, installation or performance as mentioned in RFP. Once the maximum deduction is reached, the Bank may consider termination of the Contract.

4.19 Termination for Default

4.19.1 The Bank, without prejudice to any other remedy for breach of Contract, by a written notice of default sent to the **Supplier**, may terminate the Contract in whole or in part:

- (a) if the **Supplier** fails to deliver any or all of the Products and Services, within the period(s) specified in the Contract, or within any extension thereof granted by the Bank;

OR

- (b) if the **Supplier** fails, to perform any other obligation(s) under the Contract.

4.19.2 In the event the Bank terminates the Contract in whole or in part, it may procure, up on such terms and in such manner as it deems appropriate, Products and Services similar to those undelivered, and the **Supplier** shall be liable to the Bank for any excess costs for such similar Products or Services. However, the **Supplier** shall continue performance of the Contract to the extent not terminated.

4.20 Force Majeure

- 4.20.1 Notwithstanding the provisions of TCC, the **Supplier** shall not be liable for forfeiture of its performance security, liquidated damages, or termination for default if and 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.
- 4.20.2 For purposes of this clause, “Force Majeure” means an event beyond the control of the **Supplier** and not involving the **Supplier's** fault or negligence and not foreseeable. Such events may include, but are not restricted to, acts of the Bank in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions, and freight embargoes.
- 4.20.3 If a Force Majeure situation arises, the **Supplier** shall promptly notify the Bank in writing of such condition and the cause thereof. Unless otherwise directed by the Bank in writing, the **Supplier** shall continue to perform its 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.

4.21 Termination for Insolvency

- 4.21.1 The Bank may, at any time, terminate the Contract by giving written notice to the Supplier if the Supplier becomes bankrupt or otherwise insolvent. In this event, termination will be without compensation to the Supplier, 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.

4.22 Termination for Convenience

- 4.22.1 The Bank, by written notice sent to the Supplier, may terminate the Contract, in whole or in part, at any time for its convenience. The notice of termination shall specify that termination is for the Bank's convenience, the extent to which performance of the Supplier under the Contract is terminated, and the date upon which such termination becomes effective.

4.23 Resolution of Disputes

- 4.23.1 The Bank and the Supplier shall make every effort to resolve amicably by direct informal negotiation, any disagreement or dispute arising between them under or in connection with the Contract.

4.23.2 If, the Bank and the Supplier have been unable to resolve amicably a Contract dispute even after a reasonably long period, either party may require that the dispute be referred for resolution to the formal mechanisms specified herein below. These mechanisms may include, but are not restricted to, conciliation mediated by a third party and/or adjudication in an agreed national forum.

4.23.3 The dispute resolution mechanism to be applied shall be as follows:

- (a) In case of Dispute or difference arising between the Bank and the Supplier relating to any matter arising out of or connected with this agreement, such disputes or difference shall be settled in accordance with the Arbitration and Conciliation Act, 1996. Where the value of the Contract is above Rs.1.00 Crore, the arbitral tribunal shall consist of 3 arbitrators, one each to be appointed by the Purchaser and the Supplier. The third Arbitrator shall be chosen by mutual discussion between the Purchaser and the Supplier.
- (b) Arbitration proceedings shall be held at Mumbai, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be English.
- (c) The decision of the majority of arbitrators shall be final and binding upon both parties. The cost and expenses of Arbitration proceedings will be paid as determined by the arbitral tribunal. However, the expenses incurred by each party in connection with the preparation, presentation, etc., of its proceedings as also the fees and expenses paid to the arbitrator appointed by such party or on its behalf shall be borne by each party itself; and,
- (d) Where the value of the contract is Rs.1.00 Crore and below, the disputes or differences arising shall be referred to the Sole Arbitrator. The Sole Arbitrator should be appointed by agreement between the parties.

4.24 Governing Language

4.24.1 The governing language shall be English.

4.24 Applicable Law

4.25.1 The Contract shall be interpreted in accordance with the laws of the Union of India and the Bidder shall agree to submit to the courts under whose exclusive jurisdiction the Registered Office of the Bank falls.

4.26 Addresses for Notices

4.26.1 The following shall be the address of the Bank and Supplier.

Bank's address for notice purposes:

Bank of India,
Information Technology Department, Head Office,
Star House, 8th floor,
C-4, G Block, Bandra Kurla Complex,
Mumbai - 400 051

Supplier's address for notice purposes (To be filled in by the Supplier)

.....
.....
.....

4.26.2 A notice shall be effective when delivered or on effective date of the notice whichever is later.

4.27 Taxes and Duties

4.27.1 The Supplier will be entirely responsible for all applicable taxes, duties, levies, charges, license fees, road permits, etc. in connection with delivery of products at site including incidental services and commissioning. Only Goods and Services Tax (GST) shall be exclusive as applicable.

4.27.2 Income / Corporate Taxes in India:

The Supplier shall be liable to pay all corporate taxes and income tax that shall be levied according to the laws and regulations applicable from time to time in India and the price bid by the Supplier shall include all such taxes in the contract price.

4.27.3 Tax deduction at Source:

Wherever the laws and regulations require deduction of such taxes at the source of payment, the Bank shall effect such deductions from the payment due to the Supplier. The remittance of amounts so deducted and issuance of certificate for such deductions shall be made by the Bank as per the laws and regulations in force. Nothing in the Contract shall relieve the Supplier from his responsibility to

pay any tax that may be levied in India on income and profits made by the Supplier in respect of this contract.

4.27.4 The Supplier's staff, personnel and labour will be liable to pay personal income taxes in India in respect of such of their salaries and wages as are chargeable under the laws and regulations for the time being in force, and the Supplier shall perform such duties in regard to such deductions thereof as may be imposed on him by such laws and regulations.

4.28 Supplier's Integrity

The **Supplier** is responsible for and obliged to conduct all contracted activities in accordance with the contract using state-of-the-art methods and economic principles and exercising all means available to achieve the performance specified in the Contract.

4.29 Supplier's obligations

- i. The **Supplier** is obliged to work closely with the Bank's staff, act within its own authority and abide by directives issued by the Bank and implementation activities.
- ii. The **Supplier** will abide by the job safety measures prevalent in India and will free the Bank from all demands or responsibilities arising from accidents or loss of life, the cause of which is the **Supplier's** negligence. The **Supplier** will pay all indemnities arising from such incidents and will not hold the Bank responsible or obligated.
- iii. **The Supplier** is responsible for managing the activities of its personnel or sub-contracted personnel and will hold itself responsible for any misdemeanors.
- iv. **The Supplier** will treat as confidential all data and information about the Bank, obtained in the execution of his responsibilities, in strict confidence and will not reveal such information to any other party without the prior written approval of the Bank.

4.30 Site preparation and installation

The Bank is solely responsible for the construction of the hardware site in compliance with the technical and environmental specifications. The Bank will designate the installation site before the scheduled installation date, to allow the

Supplier to perform a site inspection to verify the appropriateness of the sites before the installation / commissioning of the software.

4.31 Commissioning of Solution

The Supplier is responsible for all unpacking and installation of Products. The Supplier will test all system operations and accomplish all adjustments necessary for successful and continuous operation of the software at all installation sites.

4.32 Technical Documentation

The Technical Documentation involving detailed instruction for operation and maintenance of the hardware (if any) and software is to be delivered. The language of the documentation should be English.

4.33 Right to use defective product

If after delivery, acceptance and installation and within the guarantee and AMC period, the operation or use of the product is found to be unsatisfactory, the Bank shall have the right to continue to operate or use such product until rectification of defects, errors or omissions by partial or complete replacement is made without interfering with the Bank's operation.

4.34 Repeat Orders

4.35.1 Bank reserves the right to place repeat order/s on the bidder under the same terms and conditions within contract period from the date of acceptance of purchase order by the bidder.

4.35.3 The bank reserves the right to re-negotiate the price with the bidder for downward revision of the prices.

4.35 Limitation of Liability:

Service provider will ensure Bank's data confidentiality and shall be responsible for liability arising in case of breach of any kind of security and/or leakage of confidential customer/Bank's related information to the extent of loss so caused.

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

(i) claims that are the subject of indemnification pursuant to IPR infringement,

- (ii) damage(s) occasioned by the gross negligence, fraud or willful misconduct of Service Provider,
- (iii) damage(s) occasioned by Service Provider for breach of Confidentiality Obligations,
- (iv) When a dispute is settled by the Court of Law in India.
- (v) Loss occasioned by Non-compliance of Statutory or Regulatory Guidelines.

4.36 Indemnity

- (i) The bidder has to Indemnify the Bank, and shall keep indemnified and hold the Bank harmless from and against any and all losses, liabilities, claims, actions, costs and expenses (including attorneys' fees) and also relating to and/or resulting from or in any way arising out of any claim, suit or proceeding brought against the Bank by a third party as a result of:
- (ii) An act or omission the Company, its employees, its agents, sub-contractors in the performance of the obligations of the Company under this Agreement and/or or
- (iii) Claims against the Bank and/or any legal proceedings made by employees or other persons who are deployed by the Company and/or by any statutory/regulatory/ govt. authority and/or
- (iv) Breach of any of the material term of this Agreement and/or its Annexures or breach of any representation or warranty of the Company under this Agreement, or
- (v) Violation of the Confidentiality obligations by the Company and/or its officials/employees or any other person employed by them in connection with the Contract.
- (vi) Breach of any of the material terms of this agreement by their subcontractors, if subcontracting of any part of this agreement is permitted by Bank in writing.
- (vii) Any breach of IPR violations by the Company on material if any supplied by Company.

4.37 Confidentiality:

- (i) The Company acknowledges that in the course of performing their obligations under this Agreement, the Company shall be exposed to or acquire Confidential Information of the Bank or its customers/clients. The Company understands and acknowledges that it will be given access to such Confidential Information solely as a consequence of and pursuant to this Agreement.
- (ii) The Company will, at all times, maintain confidentiality of the Confidential Information and of this Agreement, Information of Bank including of the Bank's Customer, any business , technical, financial information / data or any other information disclosed or accessible to the Company for this project whether at the time of disclosure, designated in writing as confidential or not.
- (iii) The Company agrees to keep in confidence and not disclose to any third party and all Confidential Information available to the Company and whether such information is given in writing or oral or visual, and whether such writing is marked to indicate the claims of ownership and/or secrecy or otherwise. The Company agrees that it shall not use, nor reproduce for use in any way, any Confidential Information of the Bank except to the extent required to fulfill its obligations under the Agreement. The Company agrees to protect the Confidential Information of the Bank with at least the same standard of care and procedures used by to protect its own Confidential Information of similar importance but at all times using at least a reasonable degree of care.
- (iv) The Company shall also ensure that its officials/employees and if Company is permitted by the Bank in writing to assign, delegate or hire another person to assist it in the performance of its obligations under this Agreement, such person also shall maintain the confidentiality of the Confidential Information in the same manner as the Company is bound to maintain the confidentiality.
- (v) The provisions of this Article shall survive notwithstanding the expiration or termination of this Agreement for any reason whatsoever.
- (vi) During the Term of this Project and, if applicable, during the Reverse Transition Period, Bank grants Vendor a right to use at no cost or charge the Software licensed to the Bank, solely for the purpose of providing the Services and same should be included in commercial bid.
- (vii) The bidder shall be responsible for obtaining all necessary authorizations and consents from third party licensors of Software used by vendor in performing its obligations under this Project.

(viii) If a third party's claim endangers or disrupts the Bank's use of the Software, the Vendor shall (at no further expense, charge, fees or costs to the Bank)-

- (a) obtain a license so that the Bank may continue use of the Software in accordance with the terms of this Agreement and the license agreement; or
- (b) modify the Software without affecting the functionality of the Software in any manner so as to avoid the infringement; or
- (c) replace the Software with a compatible, functionally equivalent and non-infringing product.

4.38 Weekly Reporting and Reviewing

4.38.1 Bidder should submit a weekly report on the development of the project along with reasons of delay, if any, till date of full commissioning.

4.38.2 Periodical meetings (fortnightly and monthly) will be held at Bank's premises between the Bidder and the Bank, to review the progress and the Bidder will be required to attend all such meetings and share the minutes of meetings and subsequent progress of highlighted concerns and points of the Bank.

4.39 Independent External Monitors (IEM)

Bank of India has empanelled Independent External Monitors (IEMs) for implementation of Integrity Pact (IP) in respect of procurements as per directives received from the Central Vigilance Commission (CVC).

The details are as under –

1	2
<p>Dr. Joginder Paul Sharma, IAS (Retd.) Ex-Principal Secretary. Govt. of UP D-266, Sector-47, Noida, UP Mobile: 9650999444 e-mail: sharmajp1@gmail.com</p>	<p>Shri Ashwani Kumar Ex-CMD, Dena Bank Flat No. 101, 1st Floor Plot No. F.P. No.81, Ruby Bandra West Ruby CHSL, 29th Road, Near Duruoella Convent High School. Bandra West, Mumbai- 4000050 Email:ashwani_ashwani1@yahoo.co.in</p>

4.40 Integrity Pact

Vendors/bidders/sellers, only those who commit themselves to Integrity Pact (IP) (in Format Pre-Contract Integrity Pact Format 6.18) with the Bank, would be considered competent to participate in the bidding process. In other words, entering into this pact would be the preliminary qualification. In case of bids not accompanied with signed IP by the bidders along with the technical bid, the offers shall be summarily rejected.

IP shall cover all phases of contract i.e. from the stage of Notice Inviting Tenders (NIT)/Request for Proposals (RFP) till the conclusion of the contract i.e. final payment or the duration of warrantee/guarantee. Format of Integrity Pact is attached as per Format 6.18, for strict compliance and mandatorily to be submitted with the bid document by the bidder. The integrity Pact shall be executed on applicable stamp paper and charges of the same shall be incurred by the bidders.

PART 5: FUNCTIONAL SPECIFICATIONS

The bidder shall submit datasheet for every proposed solution as supporting document for proving the compliance confirmed by them as per technical specification as mention below. The below technical specifications are minimum and mandatory in nature. The bidder shall also extend additional features which is mandatorily required to run the solution in the big enterprise level environment without any additional cost to the bank.

The technical specification of solutions are mentioned below as –

- 5.1 Disk/folder/file/ USB encryption Solution
- 5.2 Data Classification Solution
- 5.3 Mobile Device Management Solution
- 5.4 Application Whitelisting
- 5.5 File Right Management Solution
- 5.6 Secure web gateway/web proxy solution

Note-E- essential P- preferential

5.1 Solution 1- Disk/folder/file/Removable Disk /USB Encryption

Annexure-1 Technical Specifications - Item-1 Disk/folder/file/USB Encryption						
S. N.	Technical Specification	E/P	Compliance (Yes/No)	Reference (Doc Name - Pg. No. -Sec No.)	Remarks	
1	Solution should have following features:	E				
	1. Full Disk Encryption (Drive Encryption-FDE)					-
	2. File and Folder Encryption (FFE) - Removable Media Encryption (RME) USB Encryption(UE)					-
	3. File Server					-
2	Active Directory Integration- This allows using domain user information instead of creating users manually in Encryption Solutions	E			-	
3	The solution should be capable of integrating with the following:	E				
	1. Active Directory					-
	2. LDAP					-

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



	3. File Server				
4	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	E			-
5	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 – Whereas the data is encrypted on a share on a File Server	E			-
6	Solution should work in offline mode when user cannot connect to the domain/network.	E			-
7	In event of machine failure, there should be facility to remove the hard drive from the system and extract contents by connecting to another machine	E			-
8	From recovery perspective, user should be able to get the access to machine Eg: Reset his/her credential if he/she has lost or forgotten pre-boot authentication credentials, this facility should be available in both online and offline scenarios	E			-
9	Solution should do automatic encryption and protect files by dragging them into encrypted folders	E			-
10	Allow for Segregation of roles with different access levels for administrators	E			-
11	Leverage on AD Authentication to remotely access encryption server	E			-
12	Solution should use AES 128-bit/256-bit and above encryption that is used for the full disk encryption on a computer	E			-

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



13	OEM should have their own encryption engine or should support Native Encryption and come with bundled encryption engine for the supported OS mentioned below 1. OS - 32 and 64-bit Windows Vista/7 / Windows 8.1/Windows 10 prof /MAC OEM should upgrade their deployed solution and upgrade its existing setup at bank to support higher version of OS once released, during contract period	E			-
14	Solution should support SED (Self Encrypting Drives) with support for OPAL 2.0 and above	E			-
15	Secondary/Multi Drive encryption support	E			-
16	Container/Partition Encryption Solution for removable media -Ability to encrypt removable media with container/partition encryption providing flexibility to user & protection to organizations, encryption that doesn't take up entire volume	E			-
17	Solution should be able to create Password protected encrypted container / partition with a Media Viewer for sharing information with authorized users that don't have Encryption client installed	E			-
18	Solution should be able to reset password created for removable media encryption	E			-
19	Solution should provide logs centrally and capture all filenames written to external encrypted USB media in logs.	E			-
20	Dynamic Key Provisioning - Ability to provide automated process for key creation & assigning	E			-

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



21	Auto boot - Seamless boot Up without additional authentication screen yet secure with encryption	E			-
22	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)	E			-
23	Network Pre-Boot Authentication - Ability to authenticate user through LAN N/W with AD at Boot Logon	P			
24	Wireless Pre-Boot Authentication - Ability to authenticate user through WiFi N/W with AD at Boot Logon	P			
25	Crypto erase / Remote wipe Securely erasing keys keeping Data unreadable on HDD. (HDD sanitization or Disposal policy)	E			-
26	The encrypted External Media should be accessible both on Windows and Mac operating systems	E			-
27	The Solution should be deployable using proposed patch management Tool.	E			-
28	Solution should protect data with an endpoint encryption solution that is FIPS 140-2 and above	E			-
29	Solution should be compatible and integrated with the Anti-virus solution deployed by bank	E			-
30	Solution should be capable to manage/authenticate users/systems who are not a part of AD	E			-
31	Solution should support all types of known file-systems (FAT, exFAT, NTFS)	E			-
32	Encryption Solution does not prevent repair of bad sectors on non-SED drives	E			-

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



33	OS Corruption: Recovery Tool to allow for unlocking encrypted drive to recover data without decryption	E			-
34	Solution should have the capability to roll back to the original state in case of mal-functionality	E			-
35	Solution should provide with multi-factor authentication. If not, it should be capable of integrating with other multi-factor authorization tools	E			-
36	Solution should provide support for Cards, PKI, Tokens and Biometrics at Pre- Boot Support for Smart Cards and USB tokens	E			-
37	Solution should support multiple active encryption keys at a time	P			-
38	Solution should have robust data recovery procedures where user itself can generate the password in case he/she forgets the password	P			-
39	The solution should be proposed with Premium Support i.e. One Level higher than the base level support directly from the OEM.	E			-
40	The support provided should provide a single point of contact for account management and escalation from OEM (The person should be on the payroll of OEM)	E			-
41	The support should provide direct access to product specialist from authorized contacts provided by the customer.	E			-
42	The OEM should provide a utility to collect product and system information to assist Support in diagnosing issues	E			-
43	Product upgrades should be easily be downloadable from the OEM Official Website	E			-

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



44	The OEM should provide a service which delivers the latest OEM product information by email — patch and upgrade notification; and critical alerts that require immediate attention.	E			
-----------	---	----------	--	--	--

5.2 Solution 2-Data Classification Solution

A. Technical Specification

	Technical Specification	E/P	Compliance (Yes/No)	Reference (Doc Name - Pg. No. - Sec No.)	Remarks
1	The solution should evaluates content, context, identity and other attributes of unstructured data to make classification and policy decisions.	E			
2	The solution should have a simple and a flexible policy engine to support creation of rules - For example, upon an Event where the user clicks 'Send' on an email, under the Condition one of the email recipient had a certain specific email domain, to take an Action to block the email from being sent.	E			
3	The solution should trigger policy and classification actions based on different events, such as Open, Save, Print, Forward, Close, Send, or Classification Change.	E			
4	The solution should support policy conditionality based on data attributes like content, classification, recipients, sender, author, filename, path, IP address, MAC address, modification date, file type, and location and all other parameters (i.e. File Extension/ File Access Type etc.) related to data.	E			
5	The solution should provide fine-grained control over the policy actions that apply to different use cases, such as when to classify automatically and when to prompt the user.	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



6	The solution should enable administrators to define policies with or without classification as part of the policy.	E			
7	The solution should enable administrators to combine policies to provide more fine-grained control.	E			
8	The solution should support policy nesting/hierarchy to control the flow of policy execution, making it easier to support more advanced use cases for classification and policy enforcement.	E			
9	The solution should support all the file types in the Bank's environment and should have policy migration capabilities.	E			
10	The solution should seamlessly integrate into the Bank's existing IT infrastructure and should follow the existing operational and security guidelines.	E			
11	The Solution should be scalable both horizontally & vertically.	E			
12	The solution should provide context-sensitive help throughout the user interface to support security training and help users select the correct classification and policy remediation options.	E			
	Data Classification and Identification Requirements				
13	The solution should support automated, suggested, and user-driven classification.	E			
14	The solution should support the classification of messages, calendar items, and tasks from within Microsoft Outlook 2013/ 2016/ 2019 (or higher version) or any Mail Messaging Application. It should have the forward as well as backward compatibility till the	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



	available versions in the Bank's environment.				
15	The solution should enable the classification of Word, Excel and PowerPoint documents from within Microsoft Office (all versions).	E			
16	The solution should enable the classification of any file type including custom file type used by the Bank.	E			
17	The solution should enable the classification of email on iOS and Android and any other OS mobile devices.	E			
18	The solution should provide a consistent classification user experience across applications.	E			
19	The solution should support the ability to enforce classification of email and documents.	E			
20	The solution should support the ability to classify on Send, Save/Save As, Print, New Email, Close/Open Document, and other email and document events.	E			
21	The solution should support an unlimited number of classification fields.	E			
22	The solution should support multiple classification types (i.e. dropdowns, multi-selects, date fields, and user type-in).	E			
23	The solution should support data retention and disposition tags, including date fields for retention periods.	E			
24	The solution should support hierarchical and conditional classification fields, so that the appearance of a sub-field is conditional on the value selected in the higher-level field. For example,	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



	when a user selects “Restricted,” a sub-field is presented with a list of departments including “HR Only.”				
25	The solution should prominently display classification values (easily Visible) in the Microsoft Office and Outlook ribbon and for other similar applications under the Home ribbon group.	E			
26	The solution should recognize the classification of received emails and display the classification in the Outlook ribbon.	E			
27	The solution should support icon overlays to identify the classification of files in File Explorer.	E			
28	The solution should support dynamic/tailored classification selections based on the user's Active Directory attributes or groups.	E			
29	The solution should support different classification values for different applications. This can be combined with user targeting to present detailed classification options based on application and user identity.	E			
30	The solution should support the mapping of classification schemas across the Bank.	E			
31	The solution should support the mapping of old classification values to new ones, and seamlessly update previously classified information if required.	E			
32	The solution should enable users to assign classification values via a one click classification user interface.	E			
33	The solution should enable users to assign classification values while using the Outlook 2013/2016/2019 (or higher) inline reply feature.	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



34	The solution should enable users to assign classification values to any file type by right-clicking in File Explorer and selecting one or more files.	E			
35	The solution should enable users to assign classification values to non-classified email in their inbox.	E			
36	The solution should enable users to set their most frequently used classifications as "Favorites."	E			
37	The solution should enable users to save type-in fields as Favorites so that the information needs to be typed in only once.	E			
38	The solution should provide tooltips, classification descriptions, and help page links to assist users with classification policy.	E			
39	The solution should support the use of automated classification for any classification field. These classification values can be assigned based on content, context, and/or user identity (e.g. user role).	E			
40	The solution should support the dynamic population of classification fields from sources other than the pre-configured classification schema. For example, metadata values can come from document attributes (e.g. author), environmental variables (e.g. IP or MAC address), and/or Active Directory (e.g. group, department).	E			
41	The solution should support the ability to set the classification automatically based on a series of questions presented to the user via the classification dialog.	E			
42	The solution should support the ability to ask users to confirm an automated classification value (also called "suggested classification").	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



43	The solution should support the ability to prompt users to change the default classification(s) if the default is inappropriate for the content, context, or other attributes of the email or document.	E			
44	The solution should support the ability to prompt users to classify in some cases, and use automated classification in others. For example, a default classification may be used for internal email, but users are prompted to classify for external email. Or users may be prompted to classify email only when there is an attachment.	E			
45	The solution should support the ability to scan for certain keywords and regular expressions and set the classification accordingly.	E			
46	The solution should provide the ability to automatically apply classification (and protection) as files are created, moved to, change in attributes and modified in local directories and mapped drives.	E			
47	The solution should generate metadata for all file types, including persistent, embedded metadata for many non-Office files i.e. of other extensions/ formats , including PDF, TIF,TXT, Visio, Project, images, and multimedia files ,or having similar formats	E			
48	The solution should support metadata remediation and prioritization when multiple sources of metadata are available on a file. For example, a user-applied classification may be most critical and trustworthy, while in other cases, a DLP solution's tag is treated as a preferred value.	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



49	The solution should support the creation of custom metadata for interoperability, including custom X-headers.	E			
50	The solution should support customizable visual markings in email and documents (e.g. font (name/size/features), size, color, and content).	E			
51	The solution should support customizable visual markings for TXT, HTML, RTF and plaintext email.	E			
52	The solution should support the ability to add visual markings to the top and/or bottom of an email.	E			
53	The solution should support the ability to add watermarks in Microsoft Word, Emails, and other editor applications	E			
54	The solution should support the ability to evaluate multiple email and document attributes to determine the appropriate markings.	E			
55	The solution should support the use of variables in visual markings, making it easier for administrators to support multiple use cases in one policy.	E			
56	The solution should support different visual markings for the same classification, depending on context. For example, a “Confidential” email going to internal recipients may have different markings than a “Confidential” email going to external recipients.	E			
56A	The solution should have restriction feature to send “existing Email as attachment”	E			
Data Discovery Requirements					

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



57	The solution should support the discovery and identification of large volumes of data, stored both on premise and in the cloud. This includes the scanning of network file shares, SharePoint (on premise and Online), as well as Cloud storage providers.	E			
58	The solution should provide the ability to run scheduled scans to automatically classify files based on several factors, including the file properties/attributes, content, and/or metadata.	E			
59	The solution should support the ability to automatically encrypt files. This additional layer of protection can be added based on the details of the file itself, or its location.	E			
60	The solution should support the ability to collect file information during scans, including file properties, classification (pre- and post-scan), and access controls. This data inventory identifies what the data is, where it is, and who has access to it.	E			
61	The solution should provide the ability to analyze scanning results via a built-in dashboard or third-party analytics tools to minimize data at risk, monitor classification activities, and optimize data identification policies and data storage solutions.	E			
62	The solution should support the ability to quarantine files stored inappropriately, flag files for follow-up, or take action based on results of the scan. This may include updating security policies, or re-educating users on the treatment of sensitive data.	E			
Information Protection Requirements					

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



63	The solution should provide interactive warning messages that include remediation options and URL links for additional help and information.	E			
64	The solution should consolidate all policy warnings in the same policy dialog.	E			
65	The solution should enable administrators to control whether users can override policy warnings.	E			
66	The solution should provide the ability to prompt users to enter a justification when overriding a policy warning.	E			
67	The solution should support task panel alerts to visibly remind users about security policy when handling information in Office and Outlook.	E			
68	The solution should support the use of task panel alerts, which can be applied at all times or only under certain conditions. For example, the task panel can be configured to appear when handling an Excel spreadsheet containing PII.	E			
69	The solution should support the ability for users to opt-in or opt-out of any policies that the administrator defines as optional. For example, an administrator may want to allow users to opt out of using default classifications, or allow them to opt out of email and document scanning.	E			
70	The solution should allow users to click a button to run a policy check before sending an email or continuing to compose or save a document. This enable the user to run a content scan without having to do a scan on every Save.	E			
71	The solution should provide the ability to warn/prevent users from	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



	downgrading, upgrading, or changing a classification.				
72	The solution should provide the ability to save the name of the original classifier in metadata, and to enforce policy so that only the original classifier can change the classification.	E			
73	The solution should provide the ability to warn users when sending sensitive email.	E			
74	The solution should provide the ability to warn users when opening sensitive Office documents.	E			
75	The solution should provide the ability to prevent printing of sensitive email and Office documents to specific printers.	E			
76	The solution should provide the ability to highlight sensitive information within an email so that users can remediate any policy violations before the email leaves the desktop.	E			
77	The solution should provide the ability to automatically invoke the Microsoft Office Document Inspector to remove hidden or sensitive information, such as comments, revisions, and document properties – without impacting classification-related visual markings or properties.	P			
78	The solution should provide the ability to evaluate the number of instances of sensitive data within an email or document, and then apply the appropriate policy. For example, users may be allowed to send an internal email with one credit card number, but if there is more than one credit card number, the message requires a restricted classification and will be encrypted.	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



79	The solution should provide advanced control over email attachments via policies that evaluate content, recipients, sender, classification, filename, file size, and other attributes.	E			
80	The solution should provide the ability to restrict users from sending non-classified email attachments (i.e. attachments that have no classification).	E			
81	The solution should provide the ability to present the user with a checklist of blocked attachments when a policy violation occurs, and allows the user to manually select the attachments that are allowed to bypass the policy violation. For example, the user can be shown all "Confidential" attachments and asked to confirm individual attachments before sending the email.	E			
82	The solution should provide the ability to warn/prevent email attachments for certain file types (e.g. CAD drawings), content (e.g. SSNs, credit cards), file classification (e.g. "Internal"), or filename (e.g. Report_ProjectX.pdf).	E			
83	The solution should support the scanning of zip file attachments, including the ability to evaluate individual file properties such as metadata, filename, and path (e.g. when a file is within a folder within the zip file).	E			
84	The solution should support the ability to warn or prevent users from sending password-protected Microsoft Office documents via email. (The metadata in password-protected Office documents is encrypted, so this capability provide an alternative way to enforce policy.)	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



85	The solution should support the ability to check external recipient policies via an LDAP directory instead of the corporate Active Directory.	E			
86	The solution should support the ability to restrict email based on sender. For example, one user may be authorized to send sensitive information externally, but others are not allowed to do this. The policy decision may be based on the sender's email, name, or AD attributes or group membership.	E			
87	The solution should provide the ability to present the user with a checklist of blocked recipients when a policy violation occurs, and allows the user to manually select the recipients that are allowed to bypass the policy violation. For example, the user can be shown all external recipients and asked to confirm individual recipients before sending the email.	E			
88	The solution should support the ability to automatically BCC a specified mailbox when an email triggers a policy.	E			
89	The solution should enable encryption protection of files as they are uploaded to cloud storage providers within Microsoft Office.	E			
90	The solution should provide the ability to automatically apply encryption to email, documents, and files containing PII.	E			
91	The solution should provide the ability to digitally sign emails containing links, so that the recipient knows the information can be trusted.	P			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



92	The solution should support policy combinations to enable more advanced use cases, such as checking whether a document is export-controlled, and then blocking an unauthorized user from sending the document as an attachment.	E			
93	The solution should provide the ability to secure SharePoint content based on document metadata.	E			
	Auditing and Reporting Requirements				
94	The solution should log user activity while users are handling email, documents, and files.	E			
95	The solution should generate alerts via SMS/email for health monitoring of classification products.	E			
96	The solution should log alerts when a classification add-in has been disabled or any changes to the policies or configurations have been made.	E			
97	The solution should provide flexibility to send user logs to SIEM, syslog server, text file, and Windows event logs as per the need.	E			
98	The solution should provide a reporting collector that can collect events written to the Windows event logs and record them in a central reporting database.	E			
99	The solution should provide built-in reports and dashboards to analyze user behavior and system health.	E			
100	The solution should provide a pre-built starter set of reports for the reporting database (in tab separated values/ Excel or Database format) and Views and documentation to enable customers to write their own reports.	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



101	The solution should integrate with third-party reporting to provide meaningful reports on user activity and deployment.	E			
102	The solution should provide a built-in dashboard for reviewing data discovery scanning results for user activity, deployment, data storage trends, and data inventory.	E			
Mobile Security Requirement					
103	The solution should support classification of email and documents on the following mobile devices:	E			
	· Apple iPhone and iPad with iOS 9 or later.				
	· Android phones with Android platform version 4.4 or above				
	Any other OS make/version used in mobile phones				
104	The solution should support the ability to add classification label as a customizable body tag within the email message.	E			
105	The solution should provide clear display of the documents' classification when opened.	E			
106	The solution should support bi-directional transmission of documents to SharePoint.	E			
107	The solution should provide AES-256 encryption for all documents stored on the device when the app is not in use.	E			
108	The solution should support the ability to prevent document content Print, Copy and share (including in bcc) by classification through any application.	E			
109	The solution should support the ability to prevent document upload to Dropbox/Box/SharePoint based on classification or document file format.	E			

110	The solution should support environments running Enterprise Mobility Management systems.	E			
	Configuration and Deployment Requirements				
111	The solution should provide a centralized, web-based Administration Console for classification configuration and policy management.	E			
112	The solution should support the ability to save configurations in a single configuration file.	E			
113	The solution should enable clients to retrieve configurations from file shares or web servers (HTTP or HTTPS).	E			
114	The solution should enable administrators to push client configurations to user desktops via Microsoft Group Policy and other methods.	E			
115	The solution should enable administrators to tailor configurations to individuals or groups of users via Active Directory integration.	E			
116	The solution should cache configurations locally for offline use.	E			
117	The solution should enable clients to leverage policy updates without restarting Microsoft Outlook and Office applications.	P			
118	The solution should provide the ability to deploy in silent mode so that software can be deployed and enabled in different phases.	E			
119	The solution should enable administrators to customize all user interface text strings to support different languages and terminology. This includes classification fields and values, and policy warning messages.	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



120	The solution should provide administrators with pre-built regular expressions to identify PII, such as PAN numbers, Aadhaar ID numbers, Bank account numbers and debit/credit cards number.	E			
121	The solution should work with Microsoft Office 2010 (32 and 64 bit), 2013 (32-bit and 64-bit), 2016,2019 or later version	E			
122	The solution should work on Windows 7, 8, 8.1, and 10 or Higher; and Windows Server 2008 R2, 2012, and 2012 R2,2016,2019 OR Higher	E			
123	The solution should work with in virtual machine environments including VDI, Citrix Virtual Desktop, VMWare and other virtual desktops technologies.	E			
124	The solution should include installation and configuration professional services to plan, configure, and deploy the solution on-site and transfer knowledge to the organization's personnel in order to ensure continuous operation.	E			
Integration and Interoperability Requirements					
125	The solution should integrate with third-party DLP, encryption and enterprise rights management (ERM) solutions.	E			
126	The solution should provide the ability to attach metadata to information objects, which can be leveraged by e-discovery solutions.	E			
127	The solution should provide the ability to attach metadata to information objects, which can be leveraged by third-party data loss prevention (DLP) solutions and should work even when emails and documents are protected.	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



128	The solution should provide the ability to write DLP tags.	E			
129	The solution should provide the ability to trigger encryption based on metadata. For example, if a specific keyword or pattern is found in a message, the solution can add a MAPI property with the Boolean value of “True”. The encryption solution can use the “True” MAPI property to initiate the required response.	E			
130	The solution should integrate with Microsoft SharePoint with ability to scan. For example, when the user uploads the document to SharePoint, the “Classification” column in the document library is automatically populated with “CONFIDENTIAL”.	E			
131	The solution should have capability to evaluate content, context, identity and other attributes of structured data in databases to make classification and policy decisions.	P			
132	The solution should have capability to tag structured data in databases based on evaluation of data.	P			
133	The solution should quickly identify where sensitive information is available and who is touching it. It should also help prioritize risk and remediation and should be capable of locking down the data without interrupting business.	P			

B. DATA CLASIFICATION-Data Classification Guidelines (mandatory): Solution to classify as per modules given below.

Classification	Description	Examples
RESTRICTED (Private)	Restricted information is extremely sensitive and is available only to authorized employees (individuals). The loss, corruption or disclosure of	<ul style="list-style-type: none"> All Documents pertaining to Board, Board level Committees and other Top level Committees

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



	restricted information poses a massive risk and is highly likely to result in regulatory/legal action, financial loss or damage to BOI, its clients or related parties.	<ul style="list-style-type: none"> • Unpublished Financial Information • Personally identifiable information (PII) data of Customer • Cryptographic Security Keys • Information and Correspondence mark as Private and Confidential • Employee Sensitive Information • Privilege User Password of Critical systems
CONFIDENTIAL	Confidential information is sensitive to BOI and should generally only be available to those who need to know. The loss, corruption or disclosure of confidential information poses a moderate/major risk and is likely to result in regulatory/legal action, financial loss or damage to BOI, its clients or related parties	<ul style="list-style-type: none"> • Operational Budgets • Marketing Plans • Risk, Compliance and Audit Reports • Passwords/ PINs • Payroll Data
INTERNAL	Internal information poses a minor risk, but is generally available to all personnel. Its loss, corruption or disclosure poses a minor risk and is unlikely to result in regulatory/legal action, financial loss or damage to BOI, its clients or related parties	<ul style="list-style-type: none"> • Corporate Policies • Organizational Charts • Internal Phone Directories • General Procedure Manuals • Interoffice Communications
PUBLIC	Public information is available to external parties and includes information that has been intentionally disclosed by BOI, approved by BOI for public distribution, and/or externally published. Its loss, corruption or disclosure poses an insignificant risk and will not result in regulatory/legal action, financial loss or damage to BOI, its clients or related parties	<ul style="list-style-type: none"> • Published Phone Books • Released Financials • Press Releases • Published Reports

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



<p>PERSONAL USE</p>	<p>Personal information includes user's information that may include his or her name, address, email address, phone number, race, nationality, ethnicity, color, age, sex, sexual orientation, marital status, family status, identifying number, finger prints, blood type, health care history including information on physical/mental disability, educational, financial about the individual etc., except those about other individuals. This information is not sensitive to BOI. Its loss, corruption or disclosure poses an insignificant risk and will not result in regulatory/legal action, financial loss or damage to BOI, its clients or related parties</p>	<ul style="list-style-type: none">• User's PAN Card, Aadhaar Card or any other identity proof or number• User's Mobile Bill• User's Personal Tickets• User's Educational Certificates• User's Salary Slips• User's Health Reports• Any other Personnel information of user.
--------------------------------	--	---

5.3 Solution 3- Mobile Device Management (MDM) Solution

	Technical Specification	E/P	Compliance (Yes/No)	Reference (Doc Name - Pg. No. -Sec No.)	Remarks
1	The Solution should provide the Mobile Device security centrally for all enrolled corporate-owned, employee-owned and shared devices, regardless of platform or device type.	E			
2	The solution must provide capability to wrap custom apps to provide app containerization, secure app data at rest with secure AES encryption and apply granular security policies to prevent data leakage	E			
3	The solution should be capable to support the following use cases:	E			
	1. Corporate email access through mobile devices				
	2. Protection of other mobile applications published by Bank				
4	The solution must support shared devices where a single device is shared amongst multiple users with granular security policies and configurations applied to each user independent of any other user or device wide policies	E			
5	The solution should provide a group based centralized configuration and policy management. It should provide a single console for device, app and content management. It should also support custom administrative roles.	E			
6	The solution should have the capability to integrate with the following:	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



	1. Native Applications			
	2. Active Directory			
	3. Asset management solution			
	4. Patch management solution			
	5. Ticket management tool (HPSM and or similar tools)			
	6. Microsoft Exchange 2013/2016/2029 or later version			
	7. SIEM			
	8. DLP			
	9. File Share- SharePoint			
7	The solution should provide per app VPN connection to secure communication between wrapped apps and internal network without requiring device level VPN	E		
8	The solution should support Microsoft AD credential integration and certificate based user authentication for access to container apps	E		
9	The solution should have secure multi-tiered architecture (Database server securely on internal network, not in DMZ)	E		
10	The solution should support horizontal and vertical scalability to meet Bank's future requirements	E		
11	The solution should support encryption/decryption of email attachments in transit and at rest	E		
12	The solution should support editing of Microsoft Office (Docs, Excel, etc.) documents on mobile devices	E		
13	The solution must provide the capability to securely access on-premises data including file shares and share point sites from mobile devices	E		

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



14	Email secure support for Exchange, POP, and IMAP account types	E			
15	The solution should allow administrator to deploy apps by roles and groups, and provide capabilities to collect feedback and rating for apps	E			
16	The solution should have capability to publish Bank's apps and other apps available to users via an enterprise secure app store. It should provide a way to create and manage a catalogue.	E			
17	Support all mainstream mobile and tablet Operating Systems (OS), which include iOS, Chrome, Android etc.	E			
18	The solution should support feature enabling/disabling (camera/Wi-Fi/SD Card/GPS/etc.) on profile basis or centrally or group push	E			
19	All the MDM features should be compatible with all mobile/handheld device/tablet device make/vendors like Samsung/iPhone/Microsoft Surface etc.	E			
20	The solution should support cloud based app wrapping process activity through admin console only	E			
21	The solution should support full branding of the workspace with Bank's branding	E			
22	The solution should support version upgrades/patches to applications on demand by user.	E			
23	The solution should allow whitelisting/blacklisting of applications so that only whitelisted applications are allowed to run and blacklisted	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



	applications will never be installed				
24	The solution should provide built in multi factor authentication or should have the capability to integrate with third party multi factor authentication solutions	E			
25	The solution should provide remote control capabilities for troubleshooting and admin support for all supported device platforms	E			
26	The Solution should provide a simple, consistent workflow based enrolment process for user onboarding irrespective of device platforms.	E			
27	The Solution should have ability to send enrollment message using message services, email or a custom URL etc	E			
28	The solution should limit the device registration based on LDAP OU, groups and attributes (maximum device per user)	E			
29	The solution should authenticate users against Active Directory/LDAP, one-time passcodes or Security Assertion Markup Language (SAML)	E			
30	Users should be prompted and compulsorily accept terms of usage before enrollment.	E			
31	The Solution should Create and distribute customized acceptable use policies and license agreements	E			
32	The Solution should Apply and update default device policy settings.	E			
33	The Solution should Configure email, calendar, browser, contacts, Wi-Fi and VPN profiles	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



34	The Solution should have capability to Approve or quarantine new mobile devices on the network based on pre-defines policy check.	E			
35	The Solution should have ability to restrict device features such as camera, screen capture, cloud backup etc.	E			
36	The Solution should have ability to enforce kiosk mode features. Kiosk mode means to restrict device to run approved applications only.	E			
37	The solution should provide custom secure web browser	E			
38	The solution should be capable of registering multiple devices per user	E			
39	The Solution should have mobility intelligence dashboards to:	E			
	i. Provide quick view into real-time deployment data from the admin console				
	ii. Gain a graphical summary of operations and compliance				
	iii. Provide a comprehensive list of enrolled devices and drill down into specific device and user details				
40	The solution should provide detailed hardware and software inventory reports	E			
41	The Solution should have Privacy features to block sharing of personal identifiable information from containerized areas.	P			
42	The Solution should have capability to Send commands (such as device query, clear passcode, send message, lock device, set roaming, remote view, sync device) on demand to	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



	devices to request information and perform actions/commands				
43	The Solution should have capability to Remotely locate, lock and wipe lost or stolen devices; selectively wipe corporate data while leaving personal data intact.	E			
44	The solution should support creation of automated compliance rules.	E			
45	The Solution should have capability for Setting of detailed security policies for selected devices or personal policies that span across devices	E			
46	The Solution should have capability to specify passcode policies and encryption settings	E			
47	The solution should detect and restrict jail broken and rooted devices	E			
48	The solution should discover devices that are accessing enterprise systems on IP or Hostname.	E			
49	The solution should support automatic policy control that deletes all enterprise policy, apps, and data if MDM agent is uninstalled/removed.	E			
50	The solution should have the capability to push policies using web interface and should not rely on use of scripting	E			
51	The solution should provide a centralized event log tool that captures logs from all devices and administrative events (logging, policy changes, application updates, configuration updates etc.)	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



52	The solution should be capable to push policies and manage devices in WLAN environment as well.	E			
53	The solution should manage Wi-Fi supporting and non-cellular devices as well with equal policy compliance.	E			
54	The solution should be able to define policies by device type (make/model/version) or OS (type/version).	E			
55	The solution should support checking of device policy compliance before allowing enterprise resource accesses and should support and enforce user authentication before device use.	E			
56	The solution should be capable to use existing Active Directory/LDAP certificate authorities.	E			
57	The solution should record both device and console events for integrated devices to capture detailed information for system monitoring, and provide logs view in the console and export the reports.	E			
58	The solution should provide segregation of private and corporate data such that corporate data cannot be copied from the mobile via mass media storage	E			
59	The solution should have the ability to customize MDM policy to be in line with the Bank's policies such as password policy, manage groups of devices via Active Directory (AD) etc.	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



60	The solution should have the ability to act as a trusted certificate authority for integrated devices.	E			
61	The solution should configure a device to authenticate to the Bank's network using 802.1x (with EAP-TLS) and certificate-based authentication	E			
62	The solution should support device and SIM mapping so that SIM changing may disable the functioning of the device.	E			
63	The solution should provide malware and virus protection	E			
64	The solution should have capability to grant or restrict document access from outside the container.	E			
65	The solution should have capability to place prohibited applications installed on the device in quarantine.	E			
66	The solution should integrate with third party document containers i.e. Google Drive, Dropbox, SkyDrive, etc.	E			
67	The solution should report on last-connected status, updates, and push status for integrated devices.	E			
68	The solution should provide alerts via email/SMS/reports on encountering below scenarios (but not limited to):	E			
	i. Device has not connected in a period of time				
	ii. Device has outdated policies				
	iii. Device does not have encrypted data protection				
	iv. Device does not meet minimum OS version				

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



	v. Device has an installed application that is on the disallowed applications list				
	vi. Device has an installed application that is not on the allowed applications list				
	vii. Device does not have an application that is on the required applications list				
	viii. Device has uninstalled a previously installed required application				
69	The solution should provide single sign on for native mobile apps	E			
70	The solution should have a captive portal for helping users to resolving common issues E.q. User forgetting his/her password themselves.	E			
71	The solution should restrict old/outdated/vulnerable mobile OS versions(specify mobile OS version), if required	E			

5.4 Solution - Application Whitelisting

S. N	Technical Specifications	E / P	Compliance (Yes/No)	Reference (Doc Name - Pg. No. - Sec No.)	Remarks
1	The solution should be capable of automatically accepting new software/application added which are already whitelisted through policy for connected and disconnected endpoints	E			
2	The solution should be able to push policy on systems that are outside the Bank's network	E			
3	The solution should be capable to update the existing applications on the client machines only through a trusted process/installer/hash or user.	E			
4	The solution should be capable to prevent execution of all unauthorized software, scripts, and dynamic-link libraries (DLLs) and further defends against memory exploits. It should also cover portable software/.exe / other formats	E			
5	The Endpoint Administrator Users with physical or remote access to the machine should not be able to override protection.	E			
6	The solution should be able to define specific policies for specific sets of user/groups depending upon the requirements	E			
7	The solution should be capable to augment blacklisting and real-time reputation awareness	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



8	The solution should be capable to ensure that only authorized software is allowed to run, and it cannot be tampered by any malicious software.	E			
9	The solution should have a small overhead footprint which includes: <ul style="list-style-type: none"> • Easy setup and low initial and ongoing operational overhead • No file system scanning that could impact system performance • Designed to work in disconnected and in "offline" mode 	E			-
10	The solution should be able to inventorize and report on installed software and applications on every client machine	E			-
11	The solution should be agent based /agentless solution and support following OS (but not limited to): (or higher versions) <ul style="list-style-type: none"> • Microsoft Windows 7/8.1/10 • Microsoft Windows 2008/2012 • Microsoft Windows XP/Vista • Microsoft Windows XPE • Red Hat Enterprise Linux5 	E			-
12	The solution should be capable to protect against memory based attacks and application tampering. It should also cover cases where the name of the application/application's exe is changed by the user	E			-
13	The solution should be capable to offer control over the applications, based on the information of the Applications (name, checksum, etc.)	E			-

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



14	The solution should be capable to update the whitelisted applications locally and dynamically when trusted and authorized changes are implemented. The solution should be capable to maintain whitelisting records locally so that it works in offline mode as well	E			-
15	The solution should be capable of allowing only authorized applications to run and should block any changes from being done to authorized applications, like DLL's, system files, registry etc.	E			-
16	The solution should be able to work in monitoring as well as blocking mode.	E			-
17	The solution should give granular control to block versions lower than a particular version of an application	E			-
18	The solution should be capable to support systems having with least resource consumption (i.e. thin clients and kiosk systems having min 2 GB RAM, 20 GB HD with Windows 7 or later OS etc.)	E			-
19	The solution's management console should be web based and should be capable to support use of Active Directory accounts and groups to manage roles	E			
20	The solution's management console should have the capability for separation of functions and access by roles	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



21	The solution should be capable to provide pre-defined common reports and customizable reporting	E			
22	The solution Client should be capable to co-exist with the Existing Anti-Virus Solution, and other end point clients like DLP, Patch management tool etc.	E			
23	The solution should be capable to integrate with SIEM Solution	E			
24	The solution should be capable to offer the ability to produce pre-defined and user-defined alerts via Email or SMS	E			
25	The solution should be capable to provide fault tolerance when the primary data center is down	E			
26	The solution should be capable to support reporting in CSV, XML, HTML and PDF	E			
27	The solution should be capable to offer the ability to produce pre-defined and user-defined alerts via Email or SMS	E			
28	The solution should be capable to support virtualization	E			
29	The Solution should automatically accepts new software added through authorized process	E			-
30	The Solution should be capable to deploy the policies in scheduled process or real time basis.	E			
31	The solution should support Process Blocking through Kernel and Driver level Blocking.	E			-

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



32	The Solution Should support policies based on Scoring of Applications based on Threat Intelligence inputs.	E			-
33	The Solution Should Allow or block applications using a score generated by the Threat Intelligence inputs.	E			-
34	Solution Should Match Certified Safe Software and endpoint inventory applications dynamically.	E			
35	Solution should support Permanent Trusted Level- Allows applications that match this rule to install and start any other applications	E			-
36	Solution Should support all the Browsers and their versions (admin need not find all dll/sha/path himself)	E			
37	Solution should support automatic intelligence of well-known applications and versions for Developer tools (admin need not find all dll/sha/path himself)	E			
38	Solution should support automatic intelligence of well-known applications and versions for Distributed Computing (admin need not find all dll/sha/path himself)	E			
39	Solution should support automatic intelligence of well-known applications and versions for Encryption (admin need not find all dll/sha/path himself)	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



40	Solution should support automatic intelligence of well-known applications and versions for gaming software and block based on Vendor (admin need not find all dll/sha/path himself)	E			-
41	Solution should support automatic intelligence of well-known hardware and Firmware drivers (admin need not find all dll/sha/path himself)	E			
42	Solution should support automatic intelligence of applications and versions for High Risk Applications like Key Loggers, Proxy anonymizers etc (admin need not find all dll/sha/path himself)	E			
43	Solution should support automatic intelligence of applications and versions for all well-known Instant Messengers. (admin need not find all dll/sha/path himself)	E			
44	Solution should support automatic intelligence of applications and versions for all well-known Media tools like Adobe etc(admin need not find all dll/sha/path himself)	E			-
45	Solution should support automatic intelligence of applications and versions for Mobile Sync tools like Google Sync, Itunes, Samsung PC Studio or same kind of solution etc(admin need not find all dll/sha/path himself)	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



46	Solution should support automatic intelligence of applications and versions for Online Storage like Dropbox,Google Drive,One Drive or similar solutions etc.,(admin need not find all dll/sha/path himself)	E			
47	Solution should support automatic intelligence of applications and versions for MS Applications and restrict users to a certain version(admin need not find all dll/sha/path himself)	E			-
48	Solution should support automatic intelligence of applications and versions for P2P tools (admin need not find all dll/sha/path himself)	E			
49	Solution should support automatic intelligence of applications and versions for Productivity tools like Adobe, WPS office etc (admin need not find all dll/sha/path himself)	E			-
50	Solution should support automatic intelligence of applications and versions for System applications like Download Managers, File Compression, Server Services, Software updaters (admin need not find all dll/sha/path himself)	E			
51	Solution should have capability to set up approval workflow and workflow for exception	E			-
52	The Solution should maintain Version Control of at least 5 changes (addition/deletion/modification).	P			-

5.5 Solution 5- FILE RIGHTS MANAGEMENT

	Technical Specifications	E/P	Compliance (Yes/No)	Reference (Doc Name - Pg. No. -Sec No.)	Remarks
	General Rights Management Functionality				
1	The solution should be capable to provide security of documents on desktop, laptops and file servers	E			
2	The solution should be capable to provide security of documents in emails, Microsoft Outlook /Outlook on Web (OWA)	E			
3	The solution should have the capability to restrict access/use of files by users, groups & devices	E			
4	The solution should have the capability to revoke access to the documents/files to users at any time even after delivery	E			
5	The solution should have the capability to protect documents and emails text during storage, transmission and while it is being used	E			
6	The solution should be capable to enable external users to access protected documents, including agentless access (i.e. no installation of agent required to view and edit the MS office files even without the native application as bank has no visibility of software on external vendors)	E			
7	The solution should allow the user to view the documents after initial authentication and	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



	authorization without using passwords after successful first authentication				
8	The solution should be capable to provide a mechanism to manage external users separately from the internal users via a different user repository	E			
9	The solution should be capable to share protected documents with external users by applying pre-created IRM template	E			
Supported Files Formats					
10	The solution should support dominant MS Office formats and Open Office formats; and its available versions	E			
11	The solution should support older versions of MS Office e.g. 2010 especially when sharing with external user(and higher version also)	E			
12	The solution should support most commonly used file formats like PDF, text and text based formats, and dominant image formats i.e. all file formats being used by the bank	E			
13	The solution should have the capability to protect any file format being used by the Bank	E			
Environment Support					
14	The solution should support all available versions of Windows, Linux & Mac operating systems, dominant browser technologies, native app support for mobile devices like Android, iOS and other OS.	E			
15	The solution should support available databases like	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



	Microsoft SQL and Oracle, MySQL				
16	The solution should support virtualized environments for deployment of server components as well as for creating and accessing protected documents/emails	E			
Recipient Authentication					
17	The solution should have the capability to provide integration with existing user management systems e.g. Active Directory and have built-in identity management capabilities. Such integration should only be part of on premise configuration only	E			
18	The solution should support automatic deletion/disabling of internal/external users based on changes in Identity Sources	E			
19	The solution should support integration with Single Sign On systems, external authentication systems (like Google etc.)	E			
Depth and Breadth of the Policies					
20	The solution should support highly granular rights: viewing, editing, printing, copying, forwarding, screen capture prevention (even when file opens in native application), time based expiry, and restrict access on mobile devices	E			
21	The solution should be capable to allow to copy content from protected document to a protected document only and not to an unprotected document. It should insure that copied data does not lose the	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



	associated rights to that information.				
22	The solution should have the capability to lock access to a particular machine/s, and ability to restrict access based on the location (IP address) i.e. ability to restrict access of protected content inside Bank's premise only.	E			
23	The solution should have the capability to allow document creators to assign different rights for each user or group in the same window	E			
24	The solution should have the capability to provide off-line use of protected documents; can also control the period for which the user can have offline use	E			
25	The solution should have the capability to allow enforced watermarked viewing of protected files	E			
26	The solution should be capable enough to enforce protection even when the file formats are changed (e.g. word file saved as pdf)	E			
27	The solution should allow to display dynamic watermark basis classification applied in the file	E			
28	The solution should be such that there is no single point of unprotecting the documents other the document owner	E			
Management of Rights					
29	The solution should be capable to retain rights regardless of where files are stored, transmitted, used and archived. The rights and	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



	policies on the document must apply irrespective of how the document is shared i.e. copied to USB, FTP, shared via G-drive, Dropbox etc and should be independent of the collaboration platforms				
30	The assigned rights should be dynamic; one can grant and withdraw the rights for a specific user or group for the protected document at any time without the need to recall or resend the document	E			
31	The system administrator should be able to define and control which users are allowed to define policies and can monitor these policies for compliance to the Bank's security standards. Admin/Owner of the document should also be able to transfer document ownership	E			
	File-Centric Audit and Monitoring				
32	The solution should be capable to provide web-based activity searching and reporting of user activities and admin activities	E			
33	The solution should be capable to assign specific roles that can monitor the usage of all documents within the defined hierarchy	E			
34	The audit trail should capture the person who has used the document, what has been done (un/authorized), the time, and the location. Activities can be exported to be consumed by other monitoring systems.	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



35	The Solution should be capable of records management with retention period parameterization, version control and Auditing of all changes.	E			
Access to Protected Files					
36	Basic access to protected information (for view and edit) must be available on desktops without any client installation or any required application software like Word for MS office files	E			
37	The desktop client/agent should be easy to install and should provide for offline access to protected documents	E			
38	If a user forwards a protected file to other users, there must be a system driven workflow (and not just an email) for other users to ask for permissions/rights from the owner of the file	E			
Usability					
39	The solution must be easy to use and must support existing enterprise applications	E			
40	The solution should support automation of protection including prompting users to protect content	E			
41	The Solution should be capable to transfer access related policy changes to affected documents in short span of time.				
42	The solution should have reusable rights templates to remove requirement of repeated rights setting by end users. It must also provide control over which user has	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



	access to custom and predefined templates				
43	The solution should provide search-and-browse capabilities for documents, activities, and rights templates for end users and administrators	E			
44	The solution must not require a change in user behavior. For e.g. The desktop file protection must happen at the endpoint and not by uploading the file to a central location, external user must receive email attachment that is protected and not a link etc.	E			
Integration with Ecosystem					
45	The solution should provide a framework for integration with Enterprise File Share (SharePoint) and provide generic APIs for custom application integration	E			
46	The solution should have readymade connector for integration with multiple storage devices (e.g. NetAPP, SanDisk, Hitachi etc.)	E			
47	The solution should provide connectors for integration with Data Loss Prevention (DLP) systems to apply protection based on file classification and / or specific keywords identified within the document	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



48	The solution should be capable to allow for automated folder-based protection for Bank's central file server. Folders are mapped to user's machines as local drive e.g. G:\. All files existing and newly dropped in this folder must be automatically protected with predefined policies. The user's view must not be replaced with some custom or application specific view	E			
49	The Solution should have integration with PeopleSoft HRMS & Microsoft AD for user authentication / rights management. It should also support withdrawal of access rights if employee / onsite vendor staff left the organization / transfers.	E			
Manageability and Maintainability					
50	The solution's updates etc. must be easily manageable by the IT team of the Bank	E			
51	The solution should be capable to support delegation of duties and administrative functions for efficient management	E			
52	The solution should support installation of desktop client via standard desktop/infrastructure management tools like RADIA-CAE.	E			
53	The solution should provide basic in-app troubleshooting capabilities that can be easily run by end users themselves	E			
Pre-Requisites and Dependencies					

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



54	The solution should have minimal or no dependency on other proprietary hardware/softwares on the desktop or server	E			
55	The solution should not cause conflicts with other security systems like anti-virus, anti-malware systems	E			
Flexibility					
56	The solution should support segregation of duties (defining end users, system administrators, policy administrators)	E			
57	The solution should have capability to create and apply custom FRM (File Right Management) Rules at organization level, department level, Group level or user level or any specified level as per requirements.	E			
Strength of Security					
58	The solution should have the capability to keep keys and content separate at all times	E			
59	The solution should establish communication within the system as well as with external systems over secured communication protocols like https	E			
60	The solution should be capable to provide two-factor authentication or integrate with third party authentication mechanism	E			
Licensing					
61	The solution should not require additional licenses for recipients of documents within or outside of the enterprise	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



	Vendor Outsourcing (Securing data sent to Outsource partners)				
62	The solution should be capable to provide security of information irrespective of vendor's computing environment (Storage, Network Connectivity). This will be a fully offline environment	E			
63	The solution should have the provision to lock the information to a specific device on first access	E			
64	The Solution should have capability to prohibit printing / disable copy/paste/ Screen printing for entire document or selected portions	P			

5.6 Solution 6- Secure Web gateway/ Web Proxy

	Technical Specification	E/P	Compliance (Yes/No)	Reference (Doc Name - Pg. No. -Sec No.)	Remarks
1	The Secure Web gateway solution should be on- premises appliance based designed for secure proxy and active content caching services.	E			
2	The solution shall include Web Proxy with Caching, Web Content Filtering, SSL inspection, mobile device security, URL filtering, Anti Malware, Anti-Virus, Application layer filtering, Layer 7, Application control and CASB features etc.	E			
3	The solution should be scalable to minimum 60000 users without hardware/ software upgrade over contract period i.e. the product should be scalable to 60000 users without any additional hardware requirement. Additional licenses would be procured by Bank as and when required.	E			
4	The solution must not be declared End of Life during contract period i.e. for next 5 years and end of support for next 6 years from the date of acceptance by the Bank (if Bank desires to extend the AMC for additional one year after expiry of 5 years contract). In case, OEM declares their product's end of life during the contract	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



	period, Bidder should provide upgraded version of the products without any additional cost to the Bank.				
5	All components of the solution (Proxy, web / URL filtering, Antivirus, Antimalware etc.) must be deployed in Active-Active and HA Mode.	E			
6	The Solution should support explicit, SOCKS and transparent mode on the same appliance simultaneously and on same proxy instance without having to configure transparent/explicit/socks on separate dedicated instances or appliances	E			
7	The solution should have the capability to support SOCKS proxy for integration of Legacy/Special applications of the Bank.	E			
8	The solution when deployed in-line mode should support bypass mode in case of solution failure i.e. traffic flow should not break. There should also be bypass indication to know whether bypass is active or not OR any other mode to achieve the above functionality.	E			
9	The Solution should support IP spoofing to pass client IP.	E			
10	The SSL proxy should be able to communicate using either IPv4 or IPv6, either explicitly or transparently	E			
11	The Solution should support multi tenancy for deploying reverse proxy/WAF and the forward proxy on same appliance	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



12	The solution should support Sending decrypted traffic to a Forensic or Capture Device.	E			
Proxy and Caching					
13	The solution should be a Web Proxy and should support HTTP, HTTPS, TCP Proxy, and Active FTP over HTTP, SFTP, SOCKS5 and HTTPS.	E			
14	The solution should have authentication options for users/groups, It should supports authentication and authorization of users via Integrated Windows Authentication (Kerberos), NTLM (NTLM v1 and v2 in Session Security), Open LDAP & Microsoft AD etc.	E			
15	The solution should support Multiple Auth Servers / Auth Failover using Multi Scheme Auth (NTLM and LDAP). It should also support authentication exemption	E			
16	The appliance should have inbuilt caching mechanism. The appliance should have caching capacity of minimum 500GB.	E			
17	The Solution should support quota management combined with bandwidth usage and time	E			
18	The solution should provide facilities like Quality of Service (QOS), Bandwidth management based on user/user IP address/category or Group	E			
19	The solution must identify and block Webpages with: a. Malicious JavaScript / VB Script b. Malicious (or unauthorized) ActiveX applications c. Block Potentially	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



	Harmful Programs or Software's d. Malicious executables				
20	The solution should support inbuilt SSL interception and also support SSL scanning capabilities maintaining data integrity, including decryption, re- encryption of storage keys, without processing overhead and latency.	E			
21	Minimum SSL throughput supported should be 10Gbps and 400K concurrent SSL flow states and new full SSL handshake 12500 per second	E			
22	The Solution should decrypt traffic for analysis and filtering by multiple traffic analysis devices. In an in-line configuration, and should do this in both directions using a single box, so that encrypted traffic exiting the data center can also be screened for suspect traffic that in some cases is recorded in the SSL log.	E			
23	The Solution should have the ability to customize trusted CA lists.	E			
24	The solution should have capability to read encrypted web traffic. It should decrypt inbound web traffic to Bank's external facing web servers as well as outbound web traffic generated by Bank's Internal network user community	E			
25	The solution should provide the ability to exclude data from analysis (PII, Health, Banking, etc.) for privacy purpose.	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



26	The solution should provide unencrypted traffic to DLP and third party Security Analytics/Forensics logging/IDS solutions via ICAP or dedicated TAP on the appliance	E			
27	The solution should support following cipher suite in both the SSL client and reverse proxy service-:	E			
	Encryption support for TLS 1.3, 1.2, TLS 1.1, TLS 1.0, SSLv3				
	Public Key Algorithms RSA, DHE, ECDHE				
	Symmetrical key algorithms AES, AES-GCM, 3DES, DES, RC4				
	Hashing algorithm MD5, SHA-1, SHA-2, SHA256, SHA384				
	RSA Keys 512 to 2048 bits				
Management & Administration					
28	The solution should provide centralized management capabilities which includes Universal Policy enforcement across all modules & all under platforms, devices ops. This capability should allow to write policy in a single place and deploy for consistent policy across all components.	E			
29	Sensitive configuration items, such as passwords known to the solution or RSA keys, should be either encrypted or hashed when stored on disk.	E			
30	The Solution should have API based integration with other systems like Active Directory (AD), TACACS, APT etc.	E			
Logging and Reporting					

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



31	The appliance management console should have the functionality to DENY ALL TRAFFIC control to deactivate all internet services	E			
32	Solution should provide centralized reporting and logging solution for the Web proxy/content filter to get a single, consolidated view of web access and security threats across complete environment.	E			
33	The Reporting capabilities should include following: user, group, IP statistics, bandwidth & traffic management, caching statistics, malware, content, URL triggers and events, system performance and errors	E			
34	The Solution should support for exporting of report information to HTML, PDF, and text formats	E			
Application Control					
35	The solution must provide Application Controls for applications like Facebook, Twitter, Youtube, Hotmail, GMAIL, Instagram, Whatsapp and other known applications using GUI.	E			
36	Ability to strip and replace active content (Java, Visual Basic, ActiveX), restrict uploads of information, specify user agent types and versions to control client software	E			
37	The solution should natively provide control for WebEx operations to prevent data leakage to control file sharing, desktop sharing and login controls	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



38	Should have native support for CASB application classification service. Should be able to apply Policy on groups of applications	E			
39	Administrator should be able to create bandwidth rules using various different attributes like applications, IP address, time, priority etc	E			
	Malware Detection & Prevention				
40	Solution should have native capability to provide static analysis/ Advance machine learning of its own for effective malware protection.	E			
41	The solution should provide security controls for unrated/uncategorized URL's in the form of Risk score and combine that with the content/service type to create a granular policy.	E			
42	For Effective URL Categorization solution should be able to create controls over unrated sites by combining on box Database and dynamic real time URL categorization feeds.	E			
43	Solution should support supplemental "global" White list and Blacklist of sites as defined by the administrator that take precedence over any vendor-provided rule sets	E			
44	The solution should have specific categories for website classification which includes Information Security categories, enabling effective access prevention of sites, related to: "Spam", "Phishing", "Malware", "Suspicious Content" and	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



	"Command and Control networks"				
45	The solution must support roaming users security capabilities like AV scanning, SSL interception and media/web filtering to control Remote office users	E			
46	Filtering rules should support customization based on domain users, groups, domain, categories, keywords, regular expressions, time of day, day of week, source and destination IP	E			
47	The Solution should support Immediate updates of the URL filter database available to prevent phishing and other frauds	E			
48	The Solution should provide resolution to any URL rating disputes within one service day that also accepts recommendations for categorization	E			
49	The SSL (https) Proxy should be able to Validate server certificates, including revocation checks using Certificate Revocation Lists (CRLs). The SSL (https) Proxy should be able to Check various SSL parameters such as cipher and version.	E			
50	The Solution should have capability to integrated Anti-Virus scanning capabilities to block Web-based threats including Viruses, Trojans, Worms and Spyware/Adware/Malware that results in a layered defense approach against web threats.	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



51	The solution should track and block sharing of internet access from different IP source by using same credentials	E			
52	The solution should be able to switch to DR site seamlessly. For DR Cutover no manual changes should be required at end user end.	E			
53	The solution should protect against known binary executables, script based exploits, and obfuscated code or scripts entering the network.	E			
54	The solution should be capable of blocking a list of Uniform Resource Locators (URLs) of sites and pages containing malware or linking to malware infected sites	E			
54.1	The solution should be capable of un-blocking a list of Uniform Resource Locators (URLs) , which are approved by the bank for specific set of users	E			
55	Solution should have the capability to scan https headers for any malicious code i.e. it should have the capability to decrypt and look inside the https headers so as to provide protection from https infected URLs. Also solution should have SSL decryption module license inbuilt right from the first day	E			
56	The Solution should block the display of inappropriate thumbnail images in search results and enforce safe search filtering on various well known search engines like Yahoo!®, Lycos, Ask®, Bing™, Google™ etc.	E			

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



57	The solution should have integration capability with well-known DLP solutions for data leakage protection and should support ICAP.	E			
58	The solution should support different types of compression algorithms and should scan nested compressed files.	E			
59	The Solution must support pre-defined categories and custom categories. It should be possible for the solution administrator to create new categories of URLs in the application database.	E			
60	The solution should have additional gigabit ports for redundancy if offered as appliance.	E			
61	The solution should provide feature to add Non AD Users locally manually or by importing a file (excel, text) with users IDs.	P			
62	The solution should support multiple DNS (more than two)	E			
63	The solution should create the reports with password protection before distributing the reports to authorized personnel	P			
64	The Proposed Solution must provide flexibility to define separate URL Filtering policies for roaming users from the same Management Console UI only used to configure On Premise Gateway policies.	P			
65	The proposed solution at DC, DR and BKC shall be scalable to 60,000 concurrent users at any point in time. The appliance must have the same capacity from day one.	E			

Request for Proposal for Supply, Implementation and Maintenance of IT Security Solutions



Note:- In all solutions mentioned above,

“Antivirus” means any antivirus (existing or higher version) as deployed by Bank.

“MS office” is used inter-changeably with other similar applications have same features i.e. text documents (i.e. termed as MS WORD), spreadsheet (i.e. termed as MS EXCEL) , presentations(i.e. MS PowerPoint).

“Outlook” is used inter-changeably with other similar applications have same features of Mail Messaging services.

The proposed solution should support all available versions of applications (i.e. related to MS Office, Outlook) and its future higher versions, as and when deployed by Bank.

5.7 Sizing for Solutions

Bidders have to refer to the sizing sheet while quoting for the Licenses, Solution, Software, Database, Storage and Tape requirements in the Format 6.3 – Commercial Bid.

In case of any discrepancy, Bidder have to raise the Query to the Bank and Bank will publish a corrigendum for the same which will shared with all the bidders.

Sr. No	Security Solution	Initial Licenses Required	Rate Contract for additional Quantity	High Availability/ DR Infrastructure	Storage Requirement	Other Information	Complied (Y/N)	Proposed Make / Model
1.	Disk/folder/file/USB encryption	<ul style="list-style-type: none"> Full Disk /Removable /USB encryption-7000 File shares /Servers - 100 	<ul style="list-style-type: none"> Disk /folder/ file encryption- for 1000 File shares /Servers -10 	<ul style="list-style-type: none"> Management console single at DC & DR Other Components DC in HA & DR Stand Alone 	<ul style="list-style-type: none"> 3 months on Box/On-site 9 months on Secondary 9 years tape backup 	VM(including OS & Storage), Database (in case of Oracle/SQL Server) will be provided by the Bank		
2.	Data Classification Solution	10000	1000	<ul style="list-style-type: none"> Management console single at DC & DR Other Components DC & DR Stand Alone 	<ul style="list-style-type: none"> 3 months on Box/On-site 9 months on Secondary 9 years tape backup 	VM(including OS & Storage), Database (in case of Oracle/SQL Server) will be provided		

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**

बैंक ऑफ़ इंडिया
Bank of India

BOI



Sr. No.	Security Solution	Initial Licenses Required	Rate Contract for additional Quantity	High Availability/ DR Infrastructure	Storage Requirement	Other Information	Complied (Y/N)	Proposed Make / Model
						by the Bank		
3.	Mobile Device Management (MDM)	5500	1000	<ul style="list-style-type: none"> Management console single at DC & DR Other Components DC in HA & DR Stand Alone 	<ul style="list-style-type: none"> 3 months on Box/On-site 9 months on Secondary 9 years tape backup 	VM(including OS & Storage), Database (in case of Oracle/SQL Server) will be provided by the Bank		
4.	Application Whitelisting	42000	1000	<ul style="list-style-type: none"> Management console single at DC & DR Other Components DC & DR Stand Alone 	<ul style="list-style-type: none"> 3 months on Box/On-site 9 months on Secondary 9 years tape backup 	VM(including OS & Storage), Database (in case of Oracle/SQL Server) will be provided by the Bank		
5.	File Rights Management	7000	1000	<ul style="list-style-type: none"> Management console single at DC & DR Other Components DC & DR Stand Alone 	<ul style="list-style-type: none"> 3 months on Box/On-site 9 months on Secondary 9 years tape backup 	VM(including OS & Storage), Database (in case of Oracle/SQL Server) will be provided by the Bank		
6.	Secure web gateway/web proxy solutions	20000	1000	<ul style="list-style-type: none"> 3 Proxy Setup (BKC, DC and DR) in redundancy Management console in HA at DC 	<ul style="list-style-type: none"> 3 months on Box/On-site 9 months on Secondary 9 years tape backup 	Only Database (in case of Oracle/SQL Server) will be provided by the Bank, Hardware		

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



Sr. No.	Security Solution	Initial Licenses Required	Rate Contract for additional Quantity	High Availability/ DR Infrastructure	Storage Requirement	Other Information	Complied (Y/N)	Proposed Make / Model
				and BKC & Single at DR • Other Components in HA at DC, DR and BKC and Single at DR • Note-Every box should be scalable to support 60,000 concurrent users at any point in time		/OS/Storage to be provided by bidder		

PART 6: BID FORM, PRICE SCHEDULES AND OTHER FORMATS (BF)

INDEX

FORMAT NUMBERS

- 6.1.1 Bid Form (Technical Bid)
- 6.1.2 Bid Form (Price Bid)
- 6.2 Non-Disclosure Agreement
- 6.3 Price Schedule
- 6.4 Bid Security Form
- 6.5 Contract Form
- 6.6 Performance Security Form
- 6.7 Bank Guarantee Form for Advance Payment
- 6.8 Manufacturer's Authorization Form
- 6.9 Certificate for Successful Commissioning
- 6.10 Organizational Profile
- 6.11 Service Support Details
- 6.12 Bank Guarantee against Annual Maintenance
- 6.13 Bill of Material
- 6.14 Undertaking for Support Services
- 6.15 Compliance Statement
- 6.16 Confirmation for Eligibility Criteria
- 6.17 Business rules and Terms & Conditions of Reverse Auction

- 6.18 Pre-Contract Integrity Pact
- 6.19 Undertaking of Information Security Compliance
- 6.20 Know Your Employee (KYE) Compliance
- 6.21 Undertaking of Authenticity of Solution(Hardware and Software Products)
- 6.22 Self-Declaration for Non-Blacklisting
- 6.23 Escalation Matrix of all verticals
- 6.24 Undertaking for Experience of Installation and Support of proposed Solution
- 6.25 Unconditional Acceptance of the terms and conditions TCC of the RFP
- 6.26 Software/Solution Integrity Certificate
- 6.27 Undertaking on SAST/ DAST and Application Security Clearance
- 6.28 Project Plan
- 6.29 Checklist
- 6.30 Format for Submission of Pre-Bid Queries

FORMAT – 6.1.1

**BID FORM - TECHNICAL BID
(to be included in Technical Bid Envelope)**

Date :

To:

The General Manager
Bank of India
Head Office
Information Technology Department,
8th Floor, Star House-2,
C-4, G-Block, Bandra Kurla Complex,
Bandra East, Mumbai – 400 051.

Gentlemen:

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions
Ref: Your RFP Ref: BOI:HO:IT:SS:0070 Dated: 02.05.2020 BOI:HO:IT:SS:0070
Dated: 02.05.2020

~~~~~  
Having examined the Bidding Documents, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to provide Security Solutions at Bank of India and its RRBs ., in conformity with the said Bidding documents.

We undertake, if our Bid is accepted, to deliver, install and commission the Solution in accordance with the delivery schedule specified in the Schedule of Requirements.

If our Bid is accepted, we will obtain the guarantee of a bank in a sum equivalent to 10 percent of the Contract Price for the due performance of the Contract, in the form prescribed by the Bank.

***We agree to abide by the Bid and the rates quoted therein for the orders awarded by the Bank up to the period prescribed in the Bid, which shall remain binding upon us.***

Until a formal contract is prepared and executed, this Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

**Request for Proposal for Supply,  
Implementation and Maintenance of  
IT Security Solutions**



We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".

We understand that you are not bound to accept the lowest or any Bid you may receive.

Dated this ..... day of ..... 2020

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Name)

(In the capacity of)

Duly authorised to sign Bid for and on behalf of \_\_\_\_\_

**FORMAT – 6.1.2**

**BID FORM (PRICE BID)  
(to be included in Price Bid Envelope)**

Date :.....

To:

The General Manager  
Bank of India  
Head Office  
Information Technology Department,  
8<sup>th</sup> Floor, Star House-2, C-4, G-Block,  
Bandra Kurla Complex,  
Bandra East, Mumbai – 400 051

Gentlemen:

**Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions**  
**Ref: Your RFP Ref: BOI:HO:IT:SS:0070      Dated: 02.05.202002.05.2020**

~~~~~

Having examined the Bidding Documents, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to supply and deliver the captioned solution, in conformity with the said Bidding documents as may be ascertained in accordance with the schedule of Prices attached herewith and made part of this Bid.

We undertake, if our Bid is accepted, to deliver, install and commission the system in accordance with the delivery schedule specified in the Schedule of Requirements.

If our Bid is accepted, we will obtain the guarantee of a bank in a sum equivalent to 10 percent of the Contract Price for the due performance of the Contract, in the form prescribed by the Bank.

We agree to abide by the Bid and the rates quoted therein for the orders awarded by the Bank up to the period prescribed in the Bid which shall remain binding upon us.

Until a formal contract is prepared and executed, this Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



We understand that you are not bound to accept the lowest or any Bid you may receive.

Dated this day of 2020

(Signature)

(Name)

(In the capacity of)

Duly authorised to sign Bid for and on behalf of _____

FORMAT 6.2

NON-DISCLOSURE AGREEMENT

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions
Ref: Your RFP Ref: BOI:HO:IT:SS:0070 Dated: 02.05.2020

WHEREAS, we, _____, having Registered Office at _____, hereinafter referred to as the COMPANY, are agreeable for providing Security Solutions at **Bank of India & its Associates** for Bank of India, having its registered office at Star House, C-5, G Block, Bandra Kurla Complex, Mumbai – 400 051, hereinafter referred to as the BANK and,

WHEREAS, the COMPANY understands that the information regarding purchase of security solutions at **Bank of India & its RRBs** shared by the BANK in their Request for Proposal is confidential and/or proprietary to the BANK, and

WHEREAS, the COMPANY understands that in the course of submission of the offer for the **Purchase of Security Solutions at Bank of India & its Associates** and/or in the aftermath thereof, it may be necessary that the COMPANY may perform certain jobs/duties on the Bank's properties and/or have access to certain plans, documents, approvals or information of the BANK;

NOW THEREFORE, in consideration of the foregoing, the COMPANY agrees to all of the following conditions, in order to induce the BANK to grant the COMPANY specific access to the BANK's property/information

The COMPANY will not publish or disclose to others, nor, use in any services that the COMPANY performs for others, any confidential or proprietary information belonging to the BANK, unless the COMPANY has first obtained the BANK's written Authorization to do so;

The COMPANY agrees that notes, specifications, designs, memoranda and other data shared by the BANK or, prepared or produced by the COMPANY for the purpose of submitting the offer to Purchase of Security Solutions at **Bank of India** will not be disclosed to during or subsequent to submission of the offer to the BANK, to anyone outside the BANK

The COMPANY shall not, without the BANK's written consent, disclose the contents of this Request for Proposal (Bid) or any provision thereof, or any specification, plan, pattern, sample or information (to be) furnished by or on behalf of the BANK in connection therewith, to any person(s) other than those employed/engaged by the COMPANY for the purpose of submitting the offer to the BANK and/or for the performance of the Contract in the aftermath. Disclosure to

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



any employed/engaged person(s) shall be made in confidence and shall extend only so far as necessary for the purposes of such performance.

Authorized Signatory

Name:

Designation:

Office Seal:

Place:

Date:

FORMAT – 6.3
Price Bid Format
Part I

(Include in Price Bid Only – Not to be included in Technical Bid)

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions
Ref: Your RFP Ref: BOI:HO:IT:SS:0070 Dated: 02.05.2020

The Bidder must take care in filling price information in the commercial bid, to ensure that there are no typographical or arithmetic errors. All fields must be filled up correctly. Consolidated, all-inclusive fee for the total project as specified in the Request for Proposal should be mentioned.

Part A: Solutions Cost

All Solution/Appliance/ LICENSE COST shall be of One year Comprehensive warrantee

Sr. No.	Solution/ Service	Items	Qty.	Unit Cost (in INR) (Excluding Taxes)	Total (in INR) (Excluding Taxes)
1.	Disk/folder/file / Removable Disk / USB encryption	Supply & Installation of Solution in DC & DR (with High Availability/ redundancy) with all the related required items/ accessories (including database(in case of non-Oracle/ SQL Server), software / solution/ third party product etc.) with one year Support/ warrantee (A1)	1		
		Disk /folder/file encryption- Perpetual License cost of 7000 (Full Disk Encryption / USB/ Removable Disk Encryption) Nos.(endpoints/ users), with all related required items/ accessories with One year Complete AMC, ATS, Support Back Lining with OEM, (B11)	1		

Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions



Sr. No.	Solution/ Service	Items	Qty.	Unit Cost (in INR) (Excluding Taxes)	Total (in INR) (Excluding Taxes)
		File shares /Servers – 100 (endpoints/ users) with One year Complete AMC, ATS, Support Back Lining with OEM B12	1		
		Additional Perpetual license cost of 1000 Nos.(endpoints/ users) (for Disk /folder/file encryption) with all related required items/ accessories (with One year Complete AMC, ATS, Support Back Lining with OEM) (Rate Contract) C11 Note- Per License Cost (C11) = Per License Cost as quoted in (B11)	1		
		Additional perpetual license of 10 Nos. for File shares /Servers with all related required items/ accessories (with One year Complete AMC, ATS, Support Back Lining with OEM) (Rate Contract) C12 Note- Per License Cost (C12) = Per License Cost as quoted in (B12)	1		
		Total Cost A1+B11+B12+C11+C12			X1
2.	Data Classification	Supply & Installation of Solution in DC & DR (with High Availability/ redundancy) with all the related required items/ accessories (Including database (in case of non-Oracle/ SQL Server), software / solution/ third party product etc.) with one year Support/ warrantee (A2)	1		
		Perpetual License cost of 10000 Nos.(endpoints/ users), with all related required items/	1		

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



Sr. No.	Solution/ Service	Items	Qty.	Unit Cost (in INR) (Excluding Taxes)	Total (in INR) (Excluding Taxes)
		accessories,(with One year Complete AMC, ATS, Support Back Lining with OEM)(B2)			
		Additional Perpetual license cost of 1000 Nos.(endpoints/ users), with all related required items/ accessories(with One year Complete AMC, ATS, Support Back Lining with OEM) (Rate Contract) (C2)	1		
		Note- Per License Cost (C2) = Per License Cost as quoted in (B2)			
		Total Cost A2+B2+C2			X2
3.	Mobile Device Management (MDM)	Supply & Installation of Solution in DC & DR (with High Availability/ redundancy) with all the related required items/accessories (including (including database (in case of non-Oracle/ SQL Server), software / solution/ third party product etc..) with one year Support/ warrantee (A3)	1		
		Perpetual License cost of 5500 Nos.(endpoints/ users), with all related required items/ accessories with One year Complete AMC, ATS, Support Back Lining with OEM) (B3)	1		
		Additional Perpetual license cost of 1000 Nos.(endpoints/ users), including all related required items/ accessories(with One year Complete AMC, ATS, Support Back Lining with OEM) (rate Contract) (C3)	1		
		Note-Per License Cost (C3) = Per License Cost as quoted in (B3)			

Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions



Sr. No.	Solution/ Service	Items	Qty.	Unit Cost (in INR) (Excluding Taxes)	Total (in INR) (Excluding Taxes)
		Total Cost A3+B3+C3			X3
4.	Application Whitelisting	Supply & Installation of Solution in DC & DR (with High Availability/ redundancy) with all the related required items/ accessories (including database (in case of non-Oracle/ SQL Server), software / solution/ third party product etc) with one year Support/ warrantee (A4)	1		
		Perpetual License cost of 42000 Nos.(endpoints/ users), with all related required items/ accessories (with One year Complete AMC, ATS, Support Back Lining with OEM) (B4)	1		
		Additional Perpetual license cost of 1000 Nos.(endpoints/ users), with all related required items/ accessories (with One year Complete AMC, ATS, Support Back Lining with OEM)(Rate Contract) (C4) Note- Per License Cost (C4) = Per License Cost as quoted in (B4) In case, per license cost is quoted under “C4” is higher than quoted per license cost under “B4”, then price quoted under “B4” will be considered during calculation.	1		
		Total Cost A4+B4+C4			X4
5.	File Rights Management	Supply & Installation of Solution in DC & DR (with High Availability/ redundancy) with	1		

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



Sr. No.	Solution/ Service	Items	Qty.	Unit Cost (in INR) (Excluding Taxes)	Total (in INR) (Excluding Taxes)
		all the related required accessories (including database (in case of non-Oracle/ SQL Server), software / solution/ third party product etc. (A5)			
		Perpetual License for 7000 Nos.(endpoints/ users), with all related required items/ accessories (with One year complete AMC,ATS, Support Back Lining with OEM) (B5)	1		
		Additional Perpetual License for 1000 Nos.(endpoints/ users), with all related required items/ accessories (with One year Complete AMC, ATS, Support Back Lining with OEM) (rate Contract) (C5)			
		Note- Per License Cost (C5) = Per License Cost as quoted in (B5)			
		Total Cost A5+B5+C5			X5
6.	Secure web gateway/web proxy solution (3 Proxy Setups i.e. BKC, DC, DR in redundancy)	Supply & Installation of Appliance and Solution in DC, DR and BKC (with High Availability/ redundancy) with all the related required accessories (including Hardware, OS, database (in case of non-Oracle/ SQL Server), software / solution/ third party product etc.) (A6)	1		
		Cost of 20000 Nos.(endpoints/ users), with all related required items/ accessories (with One year Complete AMC, ATS,	1		

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



Sr. No.	Solution/ Service	Items	Qty.	Unit Cost (in INR) (Excluding Taxes)	Total (in INR) (Excluding Taxes)
		Support Back Lining with OEM) (B6)			
		Additional Perpetual license cost of 1000 Nos.(endpoints/ users), with all related required items/ accessories(with One year Complete AMC, ATS, Support Back Lining with OEM) (rate Contract) (C6) Note- Per License Cost (C6) = Per License Cost as quoted in (B6)	1		
		Total Cost A6+B6+C6			X6
		Grand Total X= X1+X2+X3+X4+X5+X6			X

Important Notes:

Detailed BOM/ Specifications of all Hardware/ Software, Components as above to be attached separately in the Technical Bid (Bill of Material, Format 6.13), supported by Technical Literature/Product Catalogues/Brochures, etc. This is Mandatory.

1. Bank reserve the rights to Buy for the line items as mentioned above as full or any partial hardware and software. Bank also reserve the rights to increase the number of any line items mentioned while doing the actual procurement.
2. AMC charges to be given in the prescribed format separately.
3. Price quoted should be will be exclusive of Goods & Services tax but inclusive of all other applicable taxes.
4. In case of discrepancy between figures and words, the amount in words shall prevail.
5. No increase in costs, duties, levies, taxes, charges, etc., irrespective of reasons (including exchange rate fluctuations, etc.) whatsoever, shall be admissible during the currency of the Contract.

6. Successful bidder has to submit the OEM support certificate for all Products, Hardware and Software for releasing the payment. Bank will not release the payment until certificate from OEM will not be provided.
7. Hardware and software quoted in this bid should not be END of support during contract period.
8. For any item, the price is not quoted or cost is indicated as zero, it will be assumed that the item is provided to the bank at no cost.
9. Though, rates under “additional licenses” has been sought in multiple of 1000 licenses (Rate Contract) (considering uniformity in calculation) for each solution, Bank is not bound to procure any additional licenses, in case of no additional requirement.

However, Bank at its discretion and based on requirement, may procure in full or part thereof (not in multiple of 1000 licenses) for each / all of the solutions,

The rates under “additional licenses” or rate contract shall be same of rates as quoted for licenses to be procured during solutions procurement.

10. L1 will be declared after sum of total of format 6.3 Part I, Part II and Part III.

FORMAT – 6.3(Continued)

Part II

Price Bid Format

(Include in Price Bid Only – Not to be included in Technical Bid)

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions

Ref: Your RFP Ref: BOI:HO:IT:SS:0070

Dated: 02.05.2020

The Bidder must take care in filling price information in the commercial bid, to ensure that there are no typographical or arithmetic errors. All fields must be filled up correctly. Consolidated, all-inclusive fee for the total project as specified in the Request for Proposal should be mentioned.

Part B: AMC/ATS of Entire Solutions including all kind of licenses

Sr. No	Solution/Service	Items	AMC/ATS Price per year (in INR)(Excluding Taxes)	Total Amount of 4 years (in INR) (Excluding Taxes)
1.	Disk/folder/file/USB encryption	AMC of Solution in DC & DR (with High Availability/ redundancy) with all the related required item/accessories (including database(in case of non-Oracle/ SQL Server), software / solution/ third party product etc.) for 4 year period		
		ATS/AMC for perpetual licenses Disk /folder/file encryption- Qty-7000 (Full Disk Encryption / Removable Disk Encryption) Nos. (endpoints/ users), with all related required items/		

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



Sr. No	Solution/Service	Items	AMC/ATS Price per year (in INR)(Excluding Taxes)	Total Amount of 4 years (in INR) (Excluding Taxes)
		accessories (with 4 years Complete AMC, ATS, Support Back Lining with OEM)		
		File shares /Servers – Qty -100 (endpoints/ users) with all related required items/ accessories (with 4 years Complete AMC, ATS, Support Back Lining with OEM)		
		Total Cost		Y1
2.	Data Classification	AMC of Solution in DC & DR (with High Availability/ redundancy) with all the related required item/accessories (Including database (in case of non-Oracle/ SQL Server), software / solution/ third party product etc.) for 4 year period		

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



Sr. No	Solution/Service	Items	AMC/ATS Price per year (in INR)(Excluding Taxes)	Total Amount of 4 years (in INR) (Excluding Taxes)
		ATS/AMC for Perpetual licenses Qty-10000 Nos.(endpoints/users), with all related required items/ accessories(with 4 years Complete AMC, ATS, Support Back Lining with OEM)		
		Total Cost		Y2
3.	Mobile Device Management (MDM)	AMC of Solution in DC & DR (with High Availability/ redundancy) with all the related required items/accessories (including database (in case of non-Oracle/ SQL Server), software / solution/ third party product etc.) for 4 years period		
		ATS/AMC for Perpetual Licenses Qty- 5500 Nos. (endpoints/users), with all related required items/ accessories (with 4 years Complete AMC, ATS, Support Back Lining with OEM)		
		Total Cost		Y3
4.	Application Whitelisting	AMC of Solution in DC & DR (with High		

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



Sr. No	Solution/Service	Items	AMC/ATS Price per year (in INR)(Excluding Taxes)	Total Amount of 4 years (in INR) (Excluding Taxes)
		Availability/ redundancy) with all the related required items/accessories (including database (in case of non-Oracle/ SQL Server), software / solution/ third party product etc) for 4 years period		
		ATS/AMC for Perpetual Licenses Qty-42000 Nos.(endpoints/ users), with all related required items/ accessories (with 4 years Complete AMC, ATS, Support Back Lining with OEM)		
		Total Cost		Y4
5.	File Rights Management	AMC of Solution in DC & DR (with High Availability/ redundancy) with all the related required items/accessories (including database (in case of non-Oracle/ SQL Server), software / solution/ third party product etc.) for 4 years period		
		ATS/AMC for Perpetual Licenses		

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



Sr. No	Solution/Service	Items	AMC/ATS Price per year (in INR)(Excluding Taxes)	Total Amount of 4 years (in INR) (Excluding Taxes)
		Qty-7000 Nos.(endpoints/ users), with all related required items/ accessories ,(with 4 years Complete AMC, ATS, Support Back Lining with OEM)		
		Total Cost		Y5
6.	Secure web gateway/web proxy solution (3 Proxy Setups i.e. BKC, DC, DR in redundancy)	AMC of Solution Appliance in DC, BKC & DR (with High Availability/ redundancy) with all the related required item/accessories (including Hardware, OS, database (in case of non-Oracle/ SQL Server), software / solution/ third party product etc.) for 4 years period		
		ATS/AMC for Perpetual Licenses Qty- 20000 Nos.(endpoints/ users), with all related required items/ accessories (with 4 years Complete AMC, ATS, Support Back Lining with OEM)		
		Total Cost		Y6

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



Sr. No	Solution/Service	Items	AMC/ATS Price per year (in INR)(Excluding Taxes)	Total Amount of 4 years (in INR) (Excluding Taxes)
		Grand Total		Y
		Y= Y1+Y2+Y3+Y4+Y5+Y6		

Note:

1. **(The AMC/ATS has to be a minimum of 8 % of the cost of respective line item as per Format 6.3 Part I) (All 4 Years AMC/ATS to be same i.e. same percentage)**
2. The Bidder must take care in filling price information in the commercial bid, to ensure that there are no typographical or arithmetic errors. All fields must be filled up correctly.
3. Consolidated, all-inclusive fee for the total project as specified in the Request for Proposal should be mentioned.
4. **All Prices will be exclusive of Goods & Services tax but inclusive of all other applicable taxes.**
5. All items included in part I to be quoted in part II. Quote Functional Module-wise charges, as applicable.
6. The total support period will be five years including one year warranty.
7. Payment of support will done as per calculation of the uptime which is mentioned in relevant clause.
8. AMC will be entered into by the Bank, at its sole discretion.
9. Include all applicable Software Modules / Components items as applicable, indicated in the Price Schedule. In case of discrepancy between unit price and total price, the unit price shall prevail.
10. In case of discrepancy between figures and words, the amount in words shall prevail.

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



11. AMC charges as above will be considered for Price evaluation.
12. Bidders to strictly quote in the format and for periods as mentioned above.
13. For any item, the price is not quoted or cost is indicated as zero, it will be assumed that the item is provided to the bank at no cost.
14. AMC of the payment will be released after submission of OEM certificate for support.
15. ATS/AMC for additional procured Perpetual Licenses will be at the same rate as quoted for the base quantity. If in mid, the procurement of additional licenses is made, then pro-data basis ATS/AMC will be payable post warranty (one year) by the Bank, calculated with base as Yearly ATS/AMC cost offered on prorate basis).

Signature of Bidder: _____

Name: _____

Business address: _____

Place:

Date:

FORMAT – 6.3(Continued)

Part III

Price Bid Format

(Include in Price Bid Only – Not to be included in Technical Bid)

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions
Ref: Your RFP Ref: BOI:HO:IT:SS:0070 Dated: 02.05.2020

The Bidder must take care in filling price information in the commercial bid, to ensure that there are no typographical or arithmetic errors. All fields must be filled up correctly. Consolidated, all-inclusive fee for the total project as specified in the Request for Proposal should be mentioned.

Facility management / Operations Cost

1. Bank at its discretion, may procure all/ part-of resources (L1/L2/L3) at the price quoted in price bid format Format 6.3 **Part III**. Accordingly, payment will be made on full resources/ part-of resources count.
2. Bank at its discretion, may procure additional resources (L1/L2/L3) at the unit price quoted in price bid format Format 6.3 **Part III**, in the entire contract period.

Resource type	No. of resources (Bidder to fill this column)	Unit rate per resource per month (in INR)	Unit rate per resource per year (in INR)	Total cost for 5 years (in INR)
L1	6			
L2	5			
L3	1			
Total amount in numbers				
Total amount in words (Z)				Z

Note:

1. The total support period will be 5 years. The Unit rate will remain fixed for 5 years.

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



2. Payment of support will done as per calculation of the uptime which is mentioned in relevant clause.
3. In case of discrepancy between unit price and total price, the unit price shall prevail.
4. In case of discrepancy between figures and words, the amount in words shall prevail.
5. The scope of FMS is mentioned in FMS scope of work clause mentioned in Part-3.
6. Bidder shall ensure the required uptime of 99.90% on monthly basis. Minimum resources as per point mentioned above are to be provided in our Data Center & DR Site by the selected bidder. If any additional resources are required to maintain the uptime of 99.90%, the bidder has to provide without any extra cost to the Bank.

Place:

Signature of Bidder:

Name:

Date:

Business address:

FORMAT 6.3 (Continued)

PART IV

Price Bid Format

(Include in Price Bid Only – Not to be included in Technical Bid)

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions

Ref: Your RFP Ref: BOI:HO:IT:SS:0070

Dated: 02.05.2020

The Bidder must take care in filling price information in the commercial bid, to ensure that there are no typographical or arithmetic errors. All fields must be filled up correctly. Consolidated, all-inclusive fee for the total project as specified in the Request for Proposal should be mentioned.

The Bidder must take care in filling price information in the commercial bid, to ensure that there are no typographical or arithmetic errors. All fields must be filled up correctly. Consolidated, all-inclusive fee for the total project as specified in the Request for Proposal should be mentioned.

COMPONENTS FOR L1 CRITERIA

Sr. No	Type	Total Cost (in INR)(Excluding Taxes)
1	Solution Cost(Part I) with one year warrantee/ATS-X	
2	AMC/ATS Cost for four years(Part II)-Y	
3	Facility Management Support/ Operations Cost for 5 years(Part III)-Z	
Total Cost Of The Project (TCP) in figures		
Total Cost Of The Project (TCP) in words		X+Y+Z

Validity: The prices offered will remain valid for contract period in case of Additional Licenses & Manpower resources from the date of issue of Purchase Order.

Place:

Date:

Seal & Signature of the Vendor

Note:

1. The price so quoted, shall be valid for contract period from the date of award of Contract. Prices payable to the Supplier as stated in the Contract shall be firm and not subject to adjustment during performance of the Contract, irrespective of reasons whatsoever, including exchange rate fluctuations, changes in taxes, duties, levies, charges etc.
2. Price quoted will be exclusive of all taxes, duties, levies charges, etc. Octroi or entry-tax alone, if applicable shall be reimbursed extra at actual, against proof of payment in original by the supplier. GST/ Service tax payable if any under this contract shall be payable as applicable.
3. No increase in costs, duties, levies, taxes, charges, etc., irrespective of reasons (including exchange rate fluctuations, levy of new taxes) whatsoever, shall be admissible during the Price validity Period.
4. Annual Maintenance Contract (AMC) / Annual Technical Support (ATS) shall be for 4 years. For evaluation purpose, Final Price of items as indicated in PART IV will be considered.
5. The Annual Maintenance / Technical Support i.e. AMC/ATS, offered by the bidder should have a back to back supporting arrangement with the original suppliers or their approved business partners of the hardware or software with necessary documentary evidence thereof produced to the bank.
6. Vendor will be responsible for obtaining necessary clearance/approval from the local sales tax authorities (at destination place)
7. For any item, the price is not quoted or cost is indicated as zero, it will be assumed that the item is provided to the bank at no cost.
8. L1 will be declared after sum of total of format 6.3 Part I, Part II and Part III.

Place:

Signature of Bidder:

Date

Name:

Business Address:

FORMAT 6.4

BID SECURITY FORM

Whereas(*hereinafter called "the Bidder"*) has submitted its Bid dated (*date of submission of Bid*) for the supply of (*name and/or description of the Products/system*) (*hereinafter called "the Bid"*).

KNOW ALL PEOPLE by these presents that WE (*name of bank*) of (*name of country*), having our registered office at (*address of bank*) (*hereinafter called "the Bank"*), are bound unto (*name of Purchaser*) (*hereinafter called "the Purchaser"*) in the sum of _____ for which payment well and truly to be made to the said Purchaser, the Bank binds itself, its successors, and assigns by these presents. Sealed with the Common Seal of the said Bank this ____ day of _____ 2020.

THE CONDITIONS of this obligation are:

1. If the Bidder withdraws its Bid during the period of Bid validity specified by the Bidder on the Bid Form; or
2. If the Bidder, having been notified of the acceptance of its Bid by the Purchaser during the period of Bid validity:
 - (a) fails or refuses to execute the Contract Form if required; or
 - (b) fails or refuses to furnish the performance security, in accordance with the Instruction to Bidders.

We undertake to pay the Purchaser up to the above amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due to it, owing to the occurrence of one or both of the two conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to and including forty five (45) days after the period of the Bid validity, i.e. up to _____, and any demand in respect thereof should reach the Bank not later than the above date.

(Signature of the Bidder's Bank)

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



Note: Presence of restrictive clauses in the Bid Security Form such as suit filed clause/clause requiring the Purchaser to initiate action to enforce the claim etc., will render the Bid non-responsive.

FORMAT 6.5

CONTRACT FORM (Draft Format)

THIS AGREEMENT is executed at Mumbai on this.....day of.....

BETWEEN

BANK OF INDIA, a body corporate constituted under the Banking Companies (Acquisition and Transfer of Undertakings) Act, 1970 and having its Head Office at Star House, C – 5, 'G' Block, Bandra-Kurla Complex, Bandra (East), Mumbai – 400 051, (hereinafter referred to as the "Bank" which term shall, unless repugnant to the context or meaning hereof, be deemed to mean and include its successors-in-interest and assigns) of the ONE PART:

AND

.....(*Name of Purchaser*) (hereinafter called "the Purchaser") of the one part and (*Name of Supplier*) of (*City and Country of Supplier*) (here-in-after referred to as the "Company" or "VENDOR" which expression shall, unless repugnant to the context or meaning hereof, be deemed to mean and include its successors, Liquidators and permitted assigns), of the OTHER PART.

(The "Bank" and the "Company/VENDOR" shall, wherever the context requires, be referred collectively as "**Parties**" and individually as "**Party**" also)

WHEREAS:

- A. The Bank is a prominent nationalized bank, having been founded on September 7, 1906 and having 5100 plus branches/offices as of now in India and abroad. The Bank has implemented Core Banking Solution (CBS) and the other related functions in all Branches. These branches are controlled through 54 Zonal Offices. The Bank has a dominant presence abroad with 40 branches/ offices and three representative offices. The Bank is listed at both NSE & BSE.
- B. The BANK intends to procure a total solution for Supply, Installation, Integration, Implementation, Operations and Maintenance of Security Solutions, and integrate with Bank's existing setup (applications and hardware) for a period of 5 years for Domestic and RRB Branches as per Banks' requirement. For the said purpose, the Bank had invited Bids from Competent vendor/Company/Firm by floating Request for Proposal "RFP for Procurement of Security Solutions for Bank of India & its RRBs Ref: Your RFP Ref: BOI:HO:IT:SS:0070 Dated: **02.05.2020**". In response to the Bank's said Request for Proposal (RFP), the Company had submitted its bid. The Company has represented to the Bank that it has sufficient expertise and it is fully competent to perform the said Contract as per the scope of work and on the terms and conditions set out in this Agreement and the RFP in the sum of Rs...../- (Rupees in words)

(hereinafter called "the Contract Price"). The Company has further represented that the Company has appropriate infrastructure, human and other resources required to execute various tasks of the Contract

C. Pursuant to issuing the RFP, the Bank has short-listed the Company based on the Proposal submitted, representations and warranties made by the Company. Subsequently, the Bank has awarded the said Contract to the Company subject to the terms and conditions contained in this agreement and the RFP;

D. The Parties are desirous of recording the terms as agreed between the Parties, as set out hereunder.

NOW THEREFORE, in consideration of the foregoing and the mutual covenants and promises contained herein and other good and valuable consideration the receipt and adequacy of which is hereby acknowledged, the Parties intending to be bound legally, agree as follows:

NOW THIS AGREEMENT WITNESETH AS FOLLOWS:

1. In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the Conditions of Contract referred to.
 2. Unless otherwise specifically stated in this Agreement, time will be the essence of contract for the purpose of the obligations under this Agreement.
 3. This Agreement shall commence from _____ and continue for a period offrom the said date.
24. The following documents of RFP Ref: BOI:HO:IT:SS:0070 Dated: 30.04.2020, shall be deemed to form and be read and construed as part of this Agreement, viz.:
- a) the Bid Form and the Price Schedule submitted by the Bidder as per Format 6.3 of the RFP;
 - b) the Bill of Material as per RFP;
 - c) the Technical & Functional Specifications as per RFP;
 - d) the Terms and Conditions of Contract as per RFP Ref: BOI:HO:IT:SS:0070 Dated: 30.04.2020
 - e) the Purchaser's Notification of Award as per Letter of Intent Ref.....

- f) Schedule of Dates as per RFP;
 - g) Pre bid clarifications/corrigendum's communication shared with the bidder during the processing of the bid, published during the tender process (RFP).
 - h) Timeline for deliverables as per RFP.
5. In consideration of the payments to be made by the Purchaser to the Service Provider as hereinafter mentioned, the Service Provider hereby covenants with the Purchaser to provide the total solution for Supply, Installation, Integration, Implementation, Operations and Maintenance of Security Solutions, and integrate with Bank's existing setup (applications and hardware) for a period of 5 years for Domestic and RRB Branches as per Banks' requirement, in conformity in all respects with the provisions of the Contract.
6. The Purchaser hereby covenants to pay the Service Provider in consideration of the provision of the Products and services and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the Contract at the times and in the manner prescribed by the Contract.

IN WITNESS whereof the parties hereto have caused this Agreement to be executed in accordance with their respective laws the day and year first above written.

**Signed for
[Name Of Vendor]**

by its authorized representative:

Signature of authorized representative

Full name of authorized representative

Official company title of authorized representative

in the presence of:

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



Signature of Witness

Full name of Witness

Signed for Bank of India

by its authorized representative:

Signature of authorized representative

Full name of authorized representative

Official company title of authorized representative

in the presence of:

Signature of Witness

Full name of Witness

.....
.....
.....
.....

Address:.....

.....
.....
.....

Date :

FORMAT 6.6

FORMAT OF PERFORMANCE SECURITY/ BANK GUARANTEE

Bank Guarantee No.

Date:

Issued by.....

To,

Bank of India

(As per RFP).....

.....

WHEREAS....., having its registered office at..... (hereinafter called the "Service Provider") has undertaken, in pursuance of your RFP Reference No. Ref:Dated for Supply, Installation, Integration, Implementation, Operations and Maintenance of Security Solutions, and integrate with Bank's existing setup (applications and hardware) for Domestic , Foreign and RRB Branches as per Banks' requirement for the period specified in the RFP (hereinafter called "the Contract").

2. AND WHEREAS it has been stipulated by you in the said Contract that the Service Provider shall furnish you with a Bank Guarantee by a recognized Bank for the sum of Rs..... as security for compliance with the Service Provider's performance obligations in accordance with the said Contract.

3. AND WHEREAS wehaving our Head Office at..... and a Branch office at..... at the request of the Service Provider issue this Guarantee in your favour guaranteeing the due performance of the Service Provider of the said Contract.

4. We Bank hereby agree and affirm that we are Guarantors and responsible to you, on behalf of the Service Provider, up to a sum of Rs ... (Rupees in words) and we undertake to pay you the said amounts without demur or objection, upon your first written demand declaring the Service Provider to be in default under the said Contract. We shall pay the said amounts without cavil or argument as aforesaid, without needing to prove or to show grounds or reasons for your demand or the sum specified therein.

5. We undertake to pay you any money so demanded notwithstanding any dispute or disputes raised by the Service Provider in any suit or proceeding pending before any Court or Tribunal relating thereto our liability under this present being absolute and unequivocal.

6. We, _____ (indicate the name of bank) further agree that the guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the said Contract and that it shall continue to be enforceable till all the dues of the Bank of India under or by virtue of the said Contract have been fully paid and its claims satisfied or discharged or till Bank of India certifies that the terms and conditions of the said Contract have been fully and properly carried out by the said Service Provider and accordingly discharges this guarantee. This Guarantee shall be valid up to..... and unless a demand or claim under this guarantee is made on us in writing on or before the..... +6months we shall be discharged from all liability under this guarantee thereafter.

7. We, _____ (indicate the name of bank) further agree with Bank of India that Bank of India shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said Contract or to extend time of performance by the said Service Provider from time to time or to postpone for any time or from time to time any of the powers exercisable by Bank of India against the said Service Provider and to forbear or enforce any of the terms and conditions relating to the said Contract and we shall not be relieved from our liability by reason of any such variation, or extension being granted to the said Service Provider or for any forbearance, act or omission on the part of Bank of India or any indulgence by the Bank of India to the said Service Provider or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have effect of so relieving us.

8. This guarantee will not be discharged due to the change in our constitution or of the Service Provider.

9. We, _____ (indicate the name of bank) lastly undertake not to revoke this guarantee during its currency.

Executed at..... on this the Day of
Signature and Seal of Guarantors (Service Provider's Bank)

.....
Date.....

.....
Address:
.....

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



FORMAT 6.7

BANK GUARANTEE FOR ADVANCE PAYMENT

To: _____ (Name of Purchaser)
_____ (Address of the Purchaser)

_____ (Name of Contract)

Gentlemen:

In accordance with the provisions of the Terms and Conditions of Contract, to provide for advance payment, _____ (name and address of Supplier) (hereinafter called "the Supplier") shall deposit with _____ (name of Purchaser) a bank guarantee to guarantee his proper and faithful performance under the said Clause of the Contract in an amount of _____ (amount of guarantee* (in figures and words)).

We, the _____ (bank or financial institution), as instructed by the Supplier, agree unconditionally and irrevocably to guarantee as primary obligator and not as Surety merely, the payment to _____ (name of Purchaser) on his first demand without whatsoever right of objection on our part and without his first claim to the Supplier, in the amount not exceeding _____ (amount of guarantee* in figures and words).

We further agree that no change or addition to or other modification of the terms of the Contract to be performed thereunder or of any of the Contract documents which may be made between (name of Purchaser) and the Supplier, shall in any way release us from any liability under this guarantee, and we hereby waive notice of any such change, addition or modification.

This guarantee shall remain valid and in full effect from the date of the advance payment received by the Supplier under the contract until _____ (expected date of last delivery).

Yours truly,

Signature and seal :
Name of bank/
financial institution :
Address :
Date :

- An amount is to be inserted by the bank or financial institution representing the amount of the Advance Payment.

FORMAT 6.8

MANUFACTURERS'/PRODUCERS' AUTHORIZATION FORM

No. _____

Date:

To:

The General Manager
Bank of India
Head Office
Information Technology Department,
8th Floor, Star House-2, C-4, G-Block,
Bandra Kurla Complex,
Bandra East, Mumbai – 400 051

Dear Sir:

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions
Ref: Your RFP Ref: BOI:HO:IT:SS:0070 Dated: 02.05.2020

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

We hereby extend our full guarantee for the Solution, Products and services offered by the above firm against this Bid Invitation.

We also undertake to provide any or all of the following materials, notifications, and information pertaining to the Products(Products Name) manufactured or distributed by the Supplier :

- (a) Such Products as the Bank may opt to purchase from the Supplier, provided, that this option shall not relieve the Supplier of any warranty obligations under the Contract; and
- (b) in the event of termination of production of such Products:
 - i. notification to the Bank of the pending termination, in sufficient time to permit the Bank to procure needed requirements; and
 - ii. following such termination, furnishing at no cost to the Bank and shall be inline to

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



RFP terms. The blueprints, design documents, operations manuals, standards, source codes and specifications of the Products shall be provided to bank at no cost, if requested for ensuring business continuity.

- (c) We duly authorize the said firm to act on our behalf in fulfilling all installations, Technical support and maintenance obligations required by the contract.
- (d) In case, the bidder/supplier fails / unable to deploy the solution/ solution(s) in the stipulated timeline of RFP, we, OEM, undertake to deploy the solutions, in line with the deployment methodology as proposed during bid submission by our partner and approved by us. Thereafter, support will be provided for contract period.

Yours faithfully,

Authorized Signatory
(Name of OEM/ Producers)

Note:

- i. This letter of authority should be on the letterhead of the manufacturer and should be signed by a person competent and having the power of attorney to bind the manufacturer. It should be included by the Bidder in its Bid.
- ii. This MAF/ Undertaking letter has to be issued by every OEM / all OEMs of the solutions offered by the bidder under this RFP.

FORMAT 6.9

**PROFORMA OF CERTIFICATE FOR ISSUE BY THE PURCHASER
AFTER SUCCESSFUL COMMISSIONING OF THE SOLUTION**

Ref. No.

Date:

To,
The General Manager
Bank of India
Head Office
Information Technology Department,
8th Floor, Star House-2, C-4, G-Block,
Bandra Kurla Complex,
Bandra East, Mumbai – 400 051

Dear Sir:

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions
Ref: Your RFP Ref: BOI:HO:IT:SS:0070 Dated: 02.05.2020

Sub: Certificate of commissioning of Solution

1. This is to certify that the products / equipment as detailed below has/have been received in good condition along with all the standard and special accessories (subject to remarks in Para No. 2) in accordance with the Contract/Specifications. The same has been installed and commissioned.

a) Contract No. _____ dated _____

b) Description of the Solution _____

c) Quantity _____

d) Date of commissioning and proving test _____

2. Details of products not yet supplied and recoveries to be made on that account:

<u>S.No.</u>	<u>Description</u>	<u>Amount to be recovered</u>
--------------	--------------------	-------------------------------

3. The proving test has been done to our entire satisfaction and Staff have been trained to operate the Product.
4. The Supplier has fulfilled his contractual obligations satisfactorily*

or

The Supplier has failed to fulfil his contractual obligations with regard to the following :

- (a)
 - (b)
 - (c)
 - (d)
5. The amount of recovery on account of non-supply of Products is given under Para No. 2.
 6. The amount of recovery on account of failure of the Supplier to meet his contractual obligations is as indicated in endorsement of the letter.

Signature : _____

Name : _____

Designation with stamp: _____

* Explanatory notes for filling up the certificates:

- (a) The supplier has adhered to the time schedule specified in the contract in dispatching the Products / Manuals pursuant to Technical Specifications.
- (b) The supplier has supervised the commissioning of the solution in time i.e., within the period specified in the contract from the date of intimation by the Purchaser in respect of the installation of the Product.
- (c) Training of personnel has been done by the Supplier as specified in the contract.
- (d) In the event of Manuals having not been supplied or installation and commissioning of the Solution having been delayed on account of the Supplier, the extent of delay should always be mentioned.

FORMAT 6.10

ORGANISATIONAL PROFILE

To,

The General Manager
Bank of India
Head Office
Information Technology Department,
8th Floor, Star House-2, C-4, G-Block,
Bandra Kurla Complex,
Bandra East, Mumbai – 400 051

Dear Sir:

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions

Ref: Your RFP Ref: BOI:HO:IT:SS:0070 Dated: 02.05.2020

(Include in Technical Proposal Only – Not to be included in Price Proposal)

CONSTITUTION 1. Proprietary 2. Private Ltd. 3. Public Ltd.	:	
Established since Commercial Production of the solution on Offer started since	: :	

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



Address of Registered Office	:			
Category	:	i. Software Producer / Developer (Principal) ii. Hardware Manufacturer (Principal) iii. System Integrator / Solution Provider (Third-party) iv. Any Other (<i>please specify</i>)		
		Name	Phone Nos. (with STD Codes)	
Names of Proprietor/Partners/Directors	:	1.		
		2.		
		3.		
		4.		
Number of Engineers familiar with the solution being offered	:			
Number of Total Employees	:			
Solution being offered, sold so far to:				
Purchaser, with full address and Details of contact person (Phone, Fax and E-Mail)		Modules in Use	Date of Sale	Whether Warranty/AMC still continues
1.				
2.				

Note: Please support the above facts with documentary evidence. Please also attach Income-Tax Clearance Certificate (latest) Referral Letters from Clients mentioned above

Signature of Bidder: _____

Name : _____

Business address : _____

Place:

Date:

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



FORMAT 6.11

Service Support Details Form

Ref No.

Date-

To:
The General Manager
Bank of India
Head Office
Information Technology Department,
8th Floor, Star House-2, C-4, G-Block,
Bandra Kurla Complex,
Bandra East, Mumbai – 400 051

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions
Ref: Your RFP Ref: BOI:HO:IT:SS:0070 Dated: 02.05.2020

Dear Sir:

City / Location	Postal Address, Telephone, Fax, E-Mail and Contact Details of Support Personnel	Office Working Hours (Please mention whether the Support Agency is Owned or Franchisee arrangement)	Number of Software Engineers capable of supporting the Software being offered	Owned or Franchisee.

Signature of Bidder: _____

Name : _____

Business address : _____

Place:

Date:

FORMAT 6.12

FORMAT FOR BANK GUARANTEE AGAINST ANNUAL MAINTENANCE

(ON NON-JUDICIAL STAMP PAPER OF APPROPRIATE VALUE) (If Applicable on this RFP)

Bank Guarantee No.:

Date...

To..... (Name of the Purchaser)

Whereas..... (Name of the Supplier) hereinafter called "the Supplier" has undertaken, in pursuance of contract No..... dated..... to supply..... (Description of Products and Services) hereinafter called "the Contract".

AND WHEREAS it has been stipulated by you in the said contract that the Supplier shall furnish you with a Bank Guarantee by a recognized Bank for the sum specified therein as security for compliance with the Supplier's performance obligations under the contract for Annual Maintenance and Repairs of the entire system for next five years.

AND WHEREAS we have agreed to give the Supplier a Guarantee.

THEREFORE WE hereby affirm that we are Guarantors and responsible to you on behalf of the Supplier, up to a total of Rs..... (Amount of guarantee in words and figures) being 10% of the Contract Price and we undertake to pay you, upon your first written demand declaring the Supplier to be in default under the contract and without cavil or argument, any sum or sums within the limit of Rs. (Amount of guarantee) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

This guarantee is valid until day of

Signature and Seal of Guarantors

.....

.....

Date:

Note:

1. Suppliers should ensure that seal and code no. Of the signatory is put by the bankers, before submission of the bank guarantees.
2. Stamp paper is required for the bank guarantees issued by the banks located in india.

Format 6.13

Bill of Material

(To be included in Technical Bid)

To,

The General Manager
Bank of India
Head Office
Information Technology Department,
8th Floor, Star House-2, C-4, G-Block,
Bandra Kurla Complex,
Bandra East, Mumbai – 400 051

Dear Sir:

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions
Ref: Your RFP Ref: BOI:HO:IT:SS:0070 Dated: 02.05.2020

A) **The Bidder should provide Bill of Material for entire Solution.**

Sr. No	Description	Make	Model	Quantity

We confirm that, the quoted Bill of Material (BOM) is in compliance of all RFP terms and conditions. If it is found that “BOM” is not in compliance of any/all of the terms and conditions, at any moment, the Bank as it discretion, may reject the bid / terminate the contract without any prior notice to the bidder.

Signature of Bidder: _____

Name: _____

Business Address: _____

Place:

Date:

Format 6.14

UNDERTAKING FOR SUPPORT SERVICES

To:

The General Manager
Bank of India
Head Office
Information Technology Department,
8th Floor, Star House-2, C-4, G-Block,
Bandra Kurla Complex,
Bandra East, Mumbai – 400 051

Gentlemen,

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions
Ref: Your RFP Ref: BOI:HO:IT:SS:0070 Dated: 02.05.2020

We undertake, that adequate specialized expertise shall be made available to ensure that the support services are responsive and We accept total responsibility for the fault free operation of the solution proposed and maintenance during the support period.

We shall provide the services, system spare parts and complete maintenance of the system for a period of not less than 5 years from the date of acceptance of each site, extendable on mutual agreement.

We undertake that during support Period we will maintain an Uptime of 99.90 % on monthly basis for the entire/core solution proposed.

Dated this day of 2020

(signature)

(in the capacity of)

Duly authorized to sign Proposal for and on behalf of

Format 6.15

Compliance Statement

To,

The General Manager
Bank of India
Head Office
Information Technology Department,
8th Floor, Star House-2, C-4, G-Block,
Bandra Kurla Complex,
Bandra East, Mumbai – 400 051

Gentlemen,

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions
Ref: Your RFP Ref: BOI:HO:IT:SS:0070 Dated: 02.05.2020

We certify and agree to abide by all other clauses, terms, conditions and specifications mentioned in the RFP.

Deviations if any –

Main RFP / Annexure/Format No.	Clause / Sub Clause No.	Deviation	Specific Page no. of the Response

Signature of Authorized signatory with seal

Place:

Date:

Note: There should not be any deviations in the solution proposed by the bidder. Bidder has to give his response by writing 'NIL' in the statement. It shall be deemed that there is no deviation, irrespective of the fact whether any mention in the bid document anywhere.

Format 6.16

CONFORMITY TO ELIGIBILITY CRITERIA

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions
Ref: Your RFP Ref: BOI:HO:IT:SS:0070 Dated: 02.05.2020

Sr. No.	Eligibility Criteria	Compliance (Y/N)
1	The bidder should be a registered company in India as per Companies Act 1956 / 2013 and must be in existence for the last 5 years on the date of RFP. The Certificate of Incorporation issued by Registrar of Companies along with the copies of Memorandum and Articles of Association are required to be submitted along with the technical bid.	
2	The Bidder should have minimum annual turnover of Rs. 200 Crores in each of last three preceding three (3) financial years from i.e. FY 2016-17, FY 2017-18 and FY 2018-19. The bidder should submit audited financial statements for the respective year(s). The turnover must be the individual company turnover and not that of any group of companies. Also, the bidder should have a minimum annual turnover of 30 crores or above from Sales/Services/ Maintenance/ Facility Management of similar security solutions in each of the three (3) financial years from i.e. FY 2016-17, FY 2017-18 and FY 2018-19. A self-declaration confirming the same, duly certified by same statutory auditor (who have audited the annual financial statements) to be provided only.	
3	The Bidder should have net profit in each of last three (3) financial years from i.e. FY 2016-17, FY 2017-18 and FY 2018-19. The bidder should submit audited financial statements for the respective year(s).	
4	The bidder should be highest / premium level partner / System Integrator (SI) of OEMs with an authority to sell, upgrade supply, service and maintenance of the proposed solutions (hardware and/or software) during the entire period of contract with the Bank as on the date of RFP. Relevant Certification to be attached with the bid document.	

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



	<p>The Bidder needs to submit Manufacturer Authorization Form (MAF), having reference of this RFP, from respective OEMs stating that bidder is authorized partner/ System Integrator of OEM and is authorized to participate in this RFP.</p> <p>The bidder must submit letter from OEM confirming the “Back-to-Back” agreement / arrangement for next 5 years to Bank of India, if contract is awarded to the bidder.</p>	
5	<p>During the last 5 years, the bidder should have at least 3 years of experience in undertaking continuous Annual Technical Support (ATS) of minimum five security solutions in Banks (Public / Private) / Financial Institutions. Reference letter from such organizations regarding satisfactory services to be provided by them.</p> <p>For this, the bidder may submit the reference of more than one organizations (having reference of one or more solution implementation) to comply that bidder is having experience of successful deployment and maintenance of all solutions. The bidder is required to submit the individual experience letter with word “satisfactory services” confirming the same. Non-submission of the reference experience letter with word “satisfactory services” will not be considered.</p> <p><i>POCs done will not be treated as experience of the Bidder.</i></p>	
6	<p>During the last 5 years, the bidder should have deployed minimum five solutions out of proposed solutions in Banks (Public / Private) / Financial Institutions each having minimum business mix of Rs 2 Lakh Crores as on 31.03.2019 with similar setup and DC/DR Architecture. For this, the bidder may submit the reference of more than one organizations (having reference of one or more solution implementation) to comply that bidder is having experience of successful deployment and maintenance of all solutions. The bidder is required to submit the individual experience letter with word “satisfactory services” confirming the same. Non-submission of the reference experience letter with word “satisfactory services” will not be considered.</p>	

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**

बैंक ऑफ़ इंडिया
Bank of India **BOI**



7	All/ Proposed OEM Product(s) as solutions should have been implemented in Banks (Public / Private) / Financial Institutions each having business mix of minimum Rs. 2 Lakh Crores as on 31.03.2019 and above, earlier in the last 5 years and presently under support.	
8	<p>In the response to the RFP, both bidders i.e. OEM (in individual capacity) and OEM with SI/partner can't bid simultaneously i.e. either the OEM (Original Equipment Manufacturer) (in individual capacity) or OEM with SI/partner i.e. their authorized distributor in India can bid in the RFP.</p> <p>In case, both OEM (in individual capacity) and OEM with SI/partner submitted the bids, the bid submitted by OEM (in individual capacity) will be considered.</p>	
9	The bidder/OEM should have experience in managed security in Banks/BFSI in India and deployed minimum One SOC in India The bidder should also have own/registered support offices for TAC level Support in Mumbai and Bengaluru for after sales support services and maintenance of proposed solution, hardware and software. List of branch / support offices full details of Name, Address / Telephone Numbers should be attached.	
10	The bidder has to submit Integrity Pact (IP) duly signed by authorized signatory as per the format "Format 6.18" mentioned in the RFP, on stamped paper at the time of bid submission. The bid shall be liable for rejection in case of non-submission of IP.	
11	The Bidder should submit a Certificate from their Chartered Accountants regarding their financial capability.	
12	The Auditor/ Firm/ Company/LLP or its group company / subsidiary company / holding company /affiliate /associate company / partner should have never been black listed and/ or banned and /or barred and / or disqualified and or prohibited by SEBI and/or RBI and/or NCLT and/ or NCLAT and / or any court of law and / or quasi-judicial authority / and or any other statutory and/ or regulatory authority, in undertaking any work directly or indirectly which is required to perform as stated in this RFP and/ or issuance of any certificate of audit directly or indirectly with respect to the work sated herein the RFP.	

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**

बैंक ऑफ़ इंडिया
Bank of India

BOI



13	The bidder should submit a certificate in support of ISO 9001 in support of certification of services, and to be ensured that the certificate will remain valid for entire contract duration.	
14	The bidder must have arrangements/back to back tie-ups with OEM to undertake all software upgrades / modifications necessary to conform to any changes or modifications required by the Bank and in compliance of RBI/ regulatory compliance(in time bound manner), from time to time, during the contract period .	
15	The Proposed Security solutions is in adherence to the guidelines provided in the RBI cyber security circular no RBI/2015-16/418 dated 2nd June 2016 and its subsequent amendments (in present and in future)	
16	A summary of deployment/ implementation establishing the bidder's experience and OEM/product capability must be enclosed with the Technical Bid,	
17	For "Mobile Device Management ", the solution must be in Leaders Quadrant of Gartner Report. The necessary latest Gartner Report should be attached along with Technical bid.	
18	For "Secure web gateway/web proxy solution ", the solution must be in Leaders or Challengers Quadrant of Gartner Report. The necessary latest Gartner Report should be attached along with Technical bid.	

(Above details are MANDATORY and are to be included in technical bid. Without the above details, the Bid is liable to be rejected.)

Format 6.17

BUSINESS RULES AND TERMS & CONDITIONS OF REVERSE AUCTION

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions
Ref: Your RFP Ref: BOI:HO:IT:SS:0070 Dated: 02.05.2020

Reverse Auction event will be carried out among the Technically Qualified Bidders, for providing opportunity to the Bidders, to quote the price dynamically, for the procurement for which RFP is floated.

A) Definitions:

- 1) “Bank” means Bank of India.
- 2) “Service Provider” means the third party agency / company who has been selected by the Bank for conducting Reverse Auction.
- 3) “L1” means the Bidder who has quoted lowest price in the Reverse Auction process.
- 4) “L2” means the Bidder who has quoted second lowest price in the Reverse Auction process.

B) Eligibility of Bidders to participate in Reverse Auction:

- 1) Bidders who are technically qualified in terms of the relative Terms & Conditions of the RFP and accept the Business Rules, Terms & conditions of Reversion Auction and submit the undertakings as per Annexure-A , can only participate in Reverse Auction related to the procurement for which RFP is floated. Bidders not submitting the above undertaking or submitting with deviations / amendments thereto, will be disqualified from further evaluation / participation in the process of relevant procurement.
- 2) Bidders should ensure that they have valid digital certificate well in advance to participate in the Reverse Auction. Bank and / or Service Provider will not be responsible in case Bidder could not participate in Reverse Auction due to non-availability of valid digital certificate.

C) Training:

- 1) Bank will engage the services of Service Provider to provide necessary training to representatives of all eligible Bidders for participation in Reverse Auction. All rules & procedure related to Reverse Auction will be explained during the training.

- 2) Date, Time, Venue etc. of training will be advised at appropriate time.
- 3) Eligible Bidder / his authorized nominee has to attend the training as per the schedule and at the specified venue at the his / Bidder"s own cost.
- 4) No request from the Bidders for change in training schedule and/or venue will be entertained.
- 5) However, Bank reserves the right to postpone / change / cancel the training schedule, for whatsoever reasons, without assigning any reasons therefor, even after its communication to eligible Bidders.
- 6) Any Bidder not participating in the training process will do so at his own risk.

D) Reverse Auction Schedule:

- 1) The date and time of start of Reverse Auction and its duration of time will be informed to the eligible Bidders well in advance, at least a week before the Reverse Auction date.
- 2) Bank reserves the right to postpone / change / cancel the Reverse Auction event, even after its communication to Bidders, without assigning any reasons therefor.

E) Bidding Currency:

Bidding will be conducted in Indian Rupees (INR).

F) Start Price:

Bank will determine the Start Price for Reverse Auction –

- 1) on its own and / or;
- 2) evaluating the price band information called for separately from each eligible Bidder at appropriate time and / or;
- 3) based on the price bids received and if opened, Bank may determine the start price on the basis of the lower quote received.

G) Decremental Bid Value:

- 1) The bid decrement value will be specified by Bank before the start of Reverse Auction event. It can be a fixed amount or percentage of Start Price or both whichever is higher.
- 2) Bidder is required to quote his bid price only at a decremental value.
- 3) Bidder need not quote bid price at immediate next available lower level, but it can be even at 2/3/4 level of next available lower level .

H) Conduct of Reverse Auction event:

- 1) Reverse Auction will be conducted on a specific web portal, meant for this purpose, with the help of the Service Provider identified by the Bank.
- 2) Service Provider will make all necessary arrangement for fair and transparent conduct of Reverse Auction like hosting the web portal, imparting training to eligible Bidders etc., and finally conduct of Reverse Auction.
- 3) Bidders will be participating in Reverse Auction event from their own office / place of their choice. Internet connectivity and other paraphernalia requirements shall have to be ensured by Bidder themselves.
 - a) In the event of failure of their internet connectivity (due to any reason whatsoever it may be), it is the Bidders responsibility / decision to send fax communication immediately to Service Provider, furnishing the bid price they want to bid online, with a request to upload the faxed bid price online, so that the service provider will upload that price online on behalf of the Bidder. It shall be noted clearly that the concerned Bidder, communicating this price to service provider, has to solely ensure that the fax message is received by Service Provider in a readable / legible form and also the Bidder should simultaneously check up with Service Provider over phone about the clear receipt of the bid price faxed. It shall also be clearly understood that the Bidder shall be at liberty to send such fax communications of prices to be uploaded by Service Provider only before the closure of Reverse Auction time and under no circumstances it shall be allowed beyond the closure of Reverse Auction event time. Such Bidders have to ensure that the service provider is given reasonable time by the Bidders, to upload such faxed bid prices online and if such required time is not available at the disposal of Service Provider at the time of receipt of the fax message from the Bidders, Service Provider will not be uploading the bid prices. It is to be noted that neither the Bank nor the Service Provider will be responsible for these unforeseen circumstances.
 - b) In order to ward-off such contingent situation, Bidders are advised to make all the necessary arrangements / alternatives such as back –up power supply or

whatever required, so that they are able to circumvent such situation and still be able to participate in the reverse auction successfully. However, the vendors are requested to not to wait till the last moment to quote their bids to avoid any such complex situations. Failure of power at the premises of vendors during the Reverse auction cannot be the cause for not participating in the reverse auction. On account of this, the time for the auction cannot be extended and BANK is not responsible for such eventualities.

- 4) Bank and / or Service Provider will not have any liability to Bidders for any interruption or delay in access to site of Reverse Auction irrespective of the cause.
- 5) For making the process of Reverse Auction and its result legally binding on the participating Bidders, Service Provider will enter into an agreement with each eligible Bidder, before the start of Reverse Auction event. Without this, Bidder will not be eligible to participate in the event. The format of the agreement is as per the Annexure-C.
- 6) Bidders name will be masked in the Reverse Auction process and will be given random dummy names by the Service Provider.
- 7) Bidder / his authorised representatives will be given unique Login ID & Password by Service Provider. Bidder / his authorized representative will change the Password after the receipt of initial Password from Service Provider to ensure confidentiality. All bids made from the Login ID given to the Bidders will be deemed to have been made by the concerned Bidder / his company.
- 8) Reverse auction will be conducted as per English Reverse Auction with no tie, where more than one Bidder cannot have identical bid price.
- 9) Any bid once made by the Bidder through registered Login ID & Password, the same cannot be cancelled. The Bidder is bound to supply as per the RFP at the bid price of Reverse Auction.
- 10) Auto Bid:
 - i) Bidder can take the advantage of Auto Bid facility available in Reverse Auction system. Auto Bid feature allows Bidder to place an automated bid against other Bidders in an auction by confirming to one decrement and bid without having to enter a new price each time a competing Bidder submits a new offer.
 - ii) Auto Bid facility can be used by the Bidder only once. Bidder can at no point of time during the course of the Reverse Auction, revise / delete his Auto Bid price. Bidder has the facility to revise his Auto Bid value only prior to the start of the Reverse Auction event.

- iii) Only after the lowest price quoted by other Bidders is equal to or less than the minimum Auto Bid value put in the system by Auto Bid Bidder, he will get the option to manually bid.
- iv) If more than one Bidder opts for the Auto Bid facility and if the lowest price quoted by more than one in Auto Bid facility is same, then the Bidder who has opted for the Auto Bid facility first will get the advantage of being the “L1”, with the second bidder being “L2” at a price one decrement higher than the “L1” value and so on.
- v) If one of the Bidder has opted for the Auto Bid facility, the system automatically places a bid by conforming to one decrement from the bid that any of the other Bidders might have quoted. In such a case, if the manual Bidder directly quotes the same price as the lowest price which the Bidder who has opted for the auto bid facility, then the bid submitted by the manual Bidder would be accepted as the “L1” bid. But at that point of time onwards, the manual control of the Auto Bidder would be enabled for the Auto Bidder.
- vi) Service Provider will explain in detail about the Auto Bid during the training.

11)

Reverse Auction will be for a period of one hour with unlimited extensions. If a Bidder places a bid price in last 10 minutes of closing of the Reverse auction, the auction period shall get extended automatically for another 10 minutes(default extension period).

The reverse auction gets extended continuously whenever a bid is received in the extension period. The reverse auction shall get closed automatically, when no bid is received in an extension period.

(The time period of Reverse Auction & Maximum number of its extensions & time are subject to change and will be advised to eligible Bidders before the start of the Reverse Auction event.)

12) Bidder will be able to view the following on their screen along with the necessary fields in Reverse Auction:

- i) Opening Price
- ii) Leading / Lowest Bid Price in Auction (only total price)
- iii) Last Bid Price placed by the respective Bidder.

- 13) During Reverse Auction, if no bid price is received within the specified time, Bank, at its discretion, may decide to revise Start Price / Decremental Value / scrap the reverse auction process / proceed with conventional mode of tendering.

I) Reverse Auction Process:

- 1) At the end of Reverse Auction event Service Provider will provide the Bank all necessary details of the bid prices and reports of Reverse Auction.
- 2) Upon receipt of above information from Service Provider, Bank will evaluate the same and will decide upon the winner i.e. Successful Bidder.
- 3) Successful Bidder has to fax the duly signed filled-in prescribed format (Annexure-B) as provided on case-to-case basis to Bank within 24 hours of Reverse Auction without fail. The Original signed Annexure-B should be couriered so as to reach us within 48 hours of Reverse Auction without fail.
- 4) Any variation between the on-line Reverse Auction bid price and signed document will be considered as sabotaging the tender process and will invite disqualification of Bidder/vender to conduct business with Bank as per prevailing procedure.
- 5) Successful Bidder has to give break-up of his last/lowest bid price as per Bill of Material at the end of Reverse auction event within 2 working days without fail.
- 6) Successful Bidder is bound to supply at their final bid price of Reverse Auction. In case of back out or not supply as per the rates quoted, Bank will take appropriate action against such Bidder and / or forfeit the Bid Security amount, debar him from participating in future
- 7) In case Bank decides not to go for Reverse Auction related to the procurement for which RFP is floated and price bids if any already submitted and available with Bank shall be opened as per Bank's standard practice.

J) Bidder's Obligation:

- 1) Bidder will not involve himself or any of his representatives in Price manipulation of any kind directly or indirectly with other suppliers / Bidders
- 2) Bidder will not divulge either his Bid details or any other details of Bank to any other party without written permission from the Bank.

K) Change in Business Rules, Terms & Conditions of Reverse Auction:

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



- 1) Bank reserves the right to modify / withdraw any of the Business rules, Terms & conditions of Reverse Auction at any point of time.
- 2) Modifications of Business rules, Terms & conditions of Reverse Auction will be made available on website immediately.
- 3) Modifications made during the running of Reverse Auction event will be advised to participating Bidders immediately.

Format 6.17 Continued

Annexure-A

(to be submitted on company letter head by all Bidders participating in Reverse Auction)

To,
Bank of India

Date:

Acceptance of Reverse Auction Business Rules and Terms & conditions
in respect of Tender / RFP Ref. No. **BOI:HO:IT:SS:0070** Dated: **02.05.2020** for
Supply, Implementation and Maintenance of IT Security Solutions

=====

We refer to the captioned subject and confirm that –

- 1) The undersigned is our authorized representative.
- 2) We have accepted and abide by all Terms of captioned Tender documents and Business Rules and Terms & conditions of Reverse Auction for the procurement for which RFP is floated.
- 3) Bank and Service Provider shall not be liable & responsible in any manner whatsoever for my / our failure to access & bid in Reverse Auction due to loss of internet connectivity, electricity failure, virus attack, problems with the PC, any other unforeseen circumstances etc. before or during the auction event.
- 4) We understand that in the event we are not able to access the auction site, we may authorize Service Provider to bid on our behalf by sending a fax/email containing our offer price before the auction close time and no claim can be made by us on either Bank or Service Provider regarding any loss etc. suffered by us due to acting upon our authenticated fax/email instructions.
- 5) I / We do understand that Service Provider may bid on behalf of other Bidders as well in case of above mentioned exigencies.

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



- 6) We also confirm that we have a valid digital certificate issued by a valid Certifying Authority.
- 7) We will participate in Reverse Auction conducted by _____ (name of Service Provider) and agree to enter into an agreement with him (Service Provider) for making the process of Reverse Auction and its result legally binding on us.
- 8) We will fax/email duly signed filled-in prescribed format (Annexure-B) as provided on case-to-case basis, to Bank within 24 hours of end of Reverse Auction without fail.
- 9) We will give break-up of our last / lowest bid price as per Bill of Material at the end of Reverse Auction event within 48 hours without fail.
- 10) We undertake to supply at our final lowest bid price of Reverse Auction. In case of back out or not supply as per the rates quoted by us, Bank is free to take appropriate action against us and / or forfeit the Bid Security amount, debar us from participating in future tenders.
- 11) We nominate our official Shri _____ Designation _____ of our company to participate in Reverse Auction. We authorize Bank to issue USER ID & PASSWORD to him. His official e-mail & contact number are as under

—
Email :

Mobile :

Signature with company seal :

Name of Authorized Representative:

Designation:

Email :

Mobile :

Tel. No:

Fax No.:

Format 6.17 Continued

Annexure-B

(to be submitted / faxed/emailed by Successful Bidder of Reverse Auction within 24 hours from the end of Reverse Auction event)

To,
Bank of India

Sir,

Date :

Final / Lowest Bid Price quoted in Reverse held on _____

**in respect of Tender / RFP Ref. No. BOI:HO:IT:SS:0070 Dated: 02.05.2020 for
Supply, Implementation and Maintenance of IT Security Solutions**

=====

We confirm that the final total bid price quoted by us in the captioned Reverse Auction event for captioned tender is as under –

Rs. (in figure) : _____

Rs. (in words) : _____

We confirm that –

- 1) We enclose herewith the detailed break-up of above price as per Bill of Material
OR
 We undertake to give detailed break-up of above bid price as per Bill of Material within 48 hours from the end-of Reverse Auction event.
- 2) Any variation between the on-line Reverse Auction bid price quoted by us and this document will be considered as sabotaging the tender process and will invite disqualification of Bidder/vender to conduct business with Bank as per prevailing procedure. In such case Bank is free to take appropriate action and / or forfeit the Bid Security amount and / or debar him from participating in future
- 3) We are bound to supply at the above final bid price of Reverse Auction.
- 4) We note that in case of back out or not supply as per the above rates quoted by us, Bank will take appropriate action against us and / or forfeit our Bid Security amount and / or debar him from participating in future

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



Signature with company seal:

Name of Authorized Representative:

Designation:

Email :

Mobile :

Tel. No :

Fax No:

Format 6.17 Continued

Annexure- C: Process Compliance Form

(The Bidders are required to print this on their company's letter head and sign, stamp before faxing/emailing to Service Provider, and submitted before Reverse Auction)

To
(Name & Address of Service Provider)

Sub: Agreement to the Process related Terms and Conditions
For the Reverse Auction

Dear Sir,

This has reference to the Terms & Conditions for the Reverse Auction mentioned in the Tender document for procurement of Solution against the Tender No.

This letter is to confirm that:

- 1) The undersigned is authorized representative of the company.
- 2) We have studied the Commercial Terms and the Business rules governing the Reverse Auction and the RFP as mentioned in your letter and confirm our agreement to them.
- 3) We also confirm that we have taken the training on the auction tool and have understood the functionality of the same thoroughly.
- 4) We confirm that ____ (Bank) and ____ (Service Provider) shall not be liable & responsible in any manner whatsoever for my/our failure to access & bid on the e-auction platform due to loss of internet connectivity, electricity failure, virus attack, problems with the PC, any other unforeseen circumstances etc. before or during the auction event.
- 5) We understand that in the event we are not able to access the auction site, we may authorize ____ (Service Provider) to bid on our behalf by sending a fax/email containing our offer price before the auction close time and no claim can be made by us on either ____ (Bank) or ____ (Service Provider) regarding any loss etc. suffered by us due to acting upon our authenticated fax/email instructions.
- 6) I/we do understand that ____ (Service Provider) may bid on behalf of other Bidders as well in case of above mentioned exigencies.

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



- 7) We also confirm that we have a valid digital certificate issued by a valid Certifying Authority.
- 8) We also confirm that we will fax/email the price confirmation & break up of our quoted price as per Annexure B as requested by _____(Bank) / _____(Service Provider) within the stipulated time.

We, hereby confirm that we will honor the Bids placed by us during the auction process.

With regards,

Signature with company seal

Name –

Company / Organization –

Designation within Company / Organization –

Address of Company / Organization –

Format 6.18

PRE-CONTRACT INTEGRITY PACT

PRE-CONTRACT INTEGRITY PACT
BETWEEN
BANK OF INDIA
AND

.....

General

This pre-bid pre-contract Agreement (hereinafter called the Integrity Pact) is made on day of the month of 2018, between, on one hand, the Bank of India acting through Shri , Designation of the Officer (hereinafter called the “BUYER”, which expression shall mean and include, unless the context otherwise requires, his successors in officer and assigns) of the First Part and M/s. represented by Shri Chief Executive Officer (hereinafter called the “BIDDER/Seller” which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

WHEREAS the BUYER proposes to procure (Name of the Stores/Equipment/Item) award the contract and the BIDDER/Seller is willing to offer/has offered the stores and

WHEREAS the BIDDER is a private company / public company / Government undertaking / partnership / registered export agency, constituted in accordance with the relevant law in the matter and the BUYER is a Public Sector Undertaking Bank of India.

NOW, THEREFORE,

To avoid all forms of corruption by following a system that is fair, transparent and free from any influence / prejudice dealings prior to, during and subsequent to the currency of the contract entered into with a view to :-

Enabling the BUYER to obtain the desired said stores / equipment / work at a competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement, and

Enabling BIDDERS to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing

and other corrupt practices and the BUYER will commit to prevent corruption, in any form, by its officials by following transparent procedures.

The parties hereby agree to enter into this Integrity Pact and agree as follows.

Commitments of the BUYER

1.1 The BUYER undertakes that no official of the BUYER, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through

intermediaries, any bribe, consideration, gift, reward, favour or any material or immaterial benefit or any other advantage from the BIDDER, either for themselves or for any person, organization or third party related to the contract in exchange for an advantage in the bidding process, bid evaluation, contracting or implementation process related to the contract.

1.2 The BUYER will , during the pre-contract stage, treat all BIDDERS alike, and will provide to all BIDDERS the same information and will not provide any such information to any particular BIDDER which could afford an advantage to that particular BIDDER in comparison to other BIDDERS.

1.3 All the officials of the BUYER will report to the appropriate Government office any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach.

2 In case any such preceding misconduct on the part of such officials(s) is reported by the BIDDER to the BUYER with full and verifiable facts and the same is prima facie found to be correct by the BUYER, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by the BUYER and such a person shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the BUYER the proceedings under the contract would not be stalled.

Commitments of BIDDERS

3. The BIDDER commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of its bid or during any pre-contract or post-contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following :-

3.1 The BIDDER will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER, connected directly or indirectly with the

bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.

3.2 The BIDDER further undertakes that it has not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER or otherwise in procuring the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Government for showing or forbearing to show favour or disfavor to any person in relation to the contract or any other contract with the Government.

3.3 BIDDERS shall disclose the name and address of agents and representatives and Indian BIDDERS shall disclose their foreign principals or associates.

3.4 BIDDERS shall disclose the payments to be made by them to agents/brokers or any other intermediary, in connection with this bid/contract.

3.5 The BIDDER further confirms and declares to the BUYER that the BIDDER is the original manufactures / integrator / authorized government sponsored export entity of the stores / supplier and has not engaged any individual or firm or company whether Indian or foreign to intercede, facilitate or in any way to recommend to the BUYER or any of its functionaries, whether officially or unofficially to the award of the contract to the BIDDER nor has any amount been paid promised or intended to be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.

3.6 The BIDDER, either while presenting the bid or during pre-contract negotiations or before signing the contract, shall disclose any payments he has made, is committed to or intends to make to officials of the BUYER or their family members agents, brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.

3.7 The BIDDER will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract.

3.8 The BIDDER will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.

3.9 The BIDDER shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information provided by the BUYER as part of the business relationship, regarding plans, technical proposals and business details including information contained in any

electronic data carrier. The BIDDER also undertakes to exercise due and adequate care lest any such information is divulged.

3.10 The BIDDER commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.

3.11 The BIDDER shall not instigate or cause to instigate any third person to commit any of the actions mentioned above.

3.12 If the BIDDER or any employee of the BIDDER or any person acting on behalf of the BIDDER, either directly or indirectly, is a relative of any of the officers of the BUYER or alternatively, if any relative of an officer of the BUYER has financial interest / stake in the BIDDERS firm, the same shall be disclosed by the BIDDER at the time of filling of tender. The term relative for this purpose would be as defined in Section 6 of the Companies Act 1956.

3.13 The BIDDER shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the BUYER.

4. Previous Transgression

4.1 The BIDDER declares that no previous transgression occurred in the last three years immediately before signing of this Integrity Pact, with any other company in any country in respect of any corrupt practices envisaged hereunder or with any Public Sector Enterprise in India or any Government Department in India that could justify BIDDER's exclusion from the tender process.

4.2 The BIDDER agrees that if it makes incorrect statement on this subject, BIDDER can be disqualified from the tender process or the contract, if already awarded can be terminated for such reason.

5. Earnest Money (Security Deposit)

5.1 While submitting commercial bid, the BIDDER shall deposit an amount _____ as specified in the RFP as Earnest Money/Security Deposit, with the BUYER through any of the following instruments

- (i) Bank Draft or a Pay Order in favour of _____
- (ii) A confirmed guarantee by an Indian Nationalized Bank, promising payment of the guaranteed sum to the BUYER on demand within three working days without any demur whatsoever and without seeking any reasons whatsoever. The demand for payment by the BUYER shall be treated as conclusive proof of payment.

(iii) Any other mode or through any other instrument as specified in the RFP.

5.2 The Earnest Money / Security Deposit shall be valid upto the complete conclusion of the contractual obligations to the complete satisfaction of both the BIDDER and the BUYER, including warranty period / Defect liability period.

5.3 In case of the successful BIDDER a clause would also be incorporated in the Article pertaining to Performance Bond in the Purchase Contract that the provisions of Sanctions for Violation shall be applicable for forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

5.4 No Interest shall be payable by the BUYER to the BIDDER on Earnest Money/ Security Deposit for the period of its currency.

6. Sanctions for Violations

6.1 Any breach of the aforesaid provisions by the BIDDER or any one employed by it or acting on its behalf (Whether with or without the knowledge of the BIDDER) shall entitle the BUYER to take all or any one of the following actions, whenever required:-

- (i) To immediately call off the pre-contract negotiations without assigning any reason or giving any compensation to the BIDDER. However, the proceedings with the other BIDDER(s) would continue.
- (ii) The Earnest Money Deposit (in pre-contract stage) and / or Security Deposit / Performance Bond (after the contract is signed) shall stand forfeited either fully or partially as decided by the BUYER and the BUYER shall not be required to assign any reason therefor.
- (iii) To immediately cancel the contract if already signed, without giving any compensation to the BIDDER.
- (iv) To recover all sums already paid by the BUYER and in case of an Indian BIDDER with interest thereon at 2% higher than the prevailing Prime Lending Rate of State Bank of India, while in case of a BIDDER from a country other than India with interest thereon at 2% higher than the LIBOR. If any outstanding payment is due to the BIDDER from the BUYER in connection with any other contract for any other stores, such outstanding payment could also be utilized to recover the aforesaid sum and interest.
- (v) To encash the advance bank guarantee and performance bond / warranty bond, if furnished by the BIDDER, in order to recover the payments already made by the BUYER, along with interest.

- (vi) To cancel all or any other Contracts with the BIDDER. The BIDDER shall be liable to pay compensation for any loss or damage to the BUYER resulting from such cancellation / rescission and the BUYER shall be entitled to deduct the amount so payable from the money(s) due to the BIDDER.
- (vii) To debar the BIDDER from participating in future bidding processes of the Government of India for a minimum period of five years, which may be further extended at the discretion of the BUYER.
- (viii) To recover all sums paid in violation of this Pact by BIDDER(s) to any middlemen or agent or broker with a view to securing the contract.
- (ix) In cases where irrevocable Letters of Credit have been received in respect of any contract signed by the BUYER with the BIDDER, the same shall not be opened.
- (x) Forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

6.2 The BUYER will be entitled to take all or any of the actions mentioned at para 6.1(i) to (x) of this Pact also on the commission by the BIDDER or any one employed by it or acting on its behalf (Whether with or without the knowledge of the BIDDER), of an offence as defined in Chapter IX of the Indian Penal code, 1860 or Prevention of Corruption Act, 1988 or any other statute enacted for prevention of corruption.

6.3 The decision of the BUYER to the effect that a breach of the provisions of this Pact has been committed by the BIDDER shall be final and conclusive on the BIDDER. However, the BIDDER can approach the Independent Monitor(s) appointed for the purposes of this Pact.

7. Fail Clause

7.1 The BIDDER undertakes that it has not supplied / is not supplying similar product / systems or subsystems at a price lower than that offered in the present bid in respect of any other Ministry / Department of the Government of India or PSU and if it is found at any stage that similar product / systems or sub systems was supplied by the BIDDER to any other Ministry / Department of the Government of India or a PSU at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the BUYER, if the contract has already been concluded.

8. Independent Monitors

8.1 There shall be Independent Monitors (hereinafter referred to as Monitors) appointed by the BUYER for this Pact in consultation and with approval of the Central Vigilance Commission.

8.2 The task of the Monitors shall be to review independently and objectively whether and to what extent the parties comply with the obligations under this Pact.

8.3 The Monitors shall not be subject to instructions by the representatives of the parties and perform their functions neutrally and independently.

8.4 Both the parties accept that the Monitors have the right to access all the documents relating to the project / procurement, including minutes of meetings.

8.5 As soon as the Monitor notices, or has reason to believe, a violation of this Pact, he will so inform the Authority designated by the BUYER.

8.6 The BIDDER(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the BUYER including that provided by the BIDDER. The BIDDER will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor shall be under contractual obligation to treat the information and documents of the BIDDER / Subcontractor(s) with confidentiality.

8.7 The BUYER will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the parties. The parties will offer to the Monitor the option to participate in such meetings.

8.8 The Monitor will submit a written report to the designated Authority of BUYER within 8 to 10 weeks from the date of reference or intimation to him by the BUYER / BIDDER and, should the occasion arise, submit proposals for correcting problematic situations.

9. Facilitation of Investigation

In case of any allegation of violation of any provisions of this Pact or payment of commission, the BUYER or its agencies shall be entitled to examine all the documents including the Books of Accounts of the BIDDER and the BIDDER shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.

10. Law and Place of Jurisdiction

This Pact is subject to Indian Law. The place of performance and jurisdiction is the seat of the BUYER.

11. Other Legal Actions

The actions stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

12. Validity

12.1 The validity of this Integrity Pact shall be from date of its signing and extend upto 7 years or the complete execution of the contract to the satisfaction of both the BUYER and the BIDDER / Seller, including warranty period, whichever is later. In case BIDDER is unsuccessful, this Integrity Pact shall expire after six months from the date of the signing of the contract.

12.2 Should one or several provision of this Pact turn out to be invalid, the remainder of this Pact shall remain valid. In this case, the parties will strive to come to an agreement to their original intentions.

13. The parties hereby sign this Integrity Pact at on

BUYER

BIDDER

Name of the Officer

Name of the Officer

Designation

Designation

Bank of India

Witness

Witness

1

1

2

2

Format 6.19 - Undertaking of Information Security Compliance

**(This letter should be on the letterhead of both bidder and OEM duly
signed by an authorized signatory)**

To:
The General Manager
Bank of India
Head Office
Information Technology Department,
8th Floor, Star House-2, C-4, G-Block,
Bandra Kurla Complex,
Bandra East, Mumbai – 400 051

Sir,

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions
Ref: Your RFP Ref: Ref: BOI:HO:IT:SS:0070 Dated: 02.05.2020

We hereby undertake that the proposed solution / software to be supplied will be free of malware, free of any obvious bugs and free of any covert channels in the code (of the version of the application being delivered as well as any subsequent versions/modifications done) during entire contract period. If, any case reported, to be fixed by the bidder without any additional cost to the bank on immediate basis.

Yours faithfully,

Signature of Bidder: _____

Name: _____

Business address: _____

Place:

Date:

Format 6.20 - Know Your Employee (KYE) Compliance

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

Sir,

To:
The General Manager
Bank of India
Head Office
Information Technology Department,
8th Floor, Star House-2, C-4, G-Block,
Bandra Kurla Complex,
Bandra East, Mumbai – 400 051

Sir,

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions
Ref: Your RFP Ref: Ref: BOI:HO:IT:SS:0070 Dated: 02.05.2020

We (name of the company) hereby confirm that all the manpower (both on-site and off-site) deployed/to be deployed on Bank's project for (Name of the RFP) have undergone our internal KYE (Know Your Employee) process and requisite checks have been performed prior to employment of said employees as per our policy.

1. We undertake and agree to save defend and keep harmless and indemnified the Bank against all loss, cost, damages , claim penalties expenses, legal liability because of non-compliance of KYE and of misconduct of the employee deployed by us to the Bank.

2. We further agree to submit the required supporting documents (Process of screening, Background verification report, police verification report(issued in last six months), character certificate regarding fit and satisfactory conduct, ID card copy, Educational document, etc) to Bank before deploying officials in Bank premises for (Name of the RFP).”

Yours faithfully,

Signature of Bidder: _____
Name: _____
Business address: _____
Place: _____
Date

Format 6.21 - Undertaking of Authenticity of Solution (Hardware and Software)

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

To,

The General Manager
Bank of India
Head Office
Information Technology Department,
8th Floor, Star House-2, C-4, G-Block,
Bandra Kurla Complex,
Bandra East, Mumbai – 400 051

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions
Ref: Your RFP Ref: Ref: BOI:HO:IT:SS:0070 Dated: 02.05.2020

Dear Sir,

With reference to the subject matter, we hereby undertake that all the components/parts/assembly/software used in the Solution, Hardware, Application Server Software and Backup software for Proposed Solutions shall be original and new components / products only, from respective OEMs of the products and that no refurbished / duplicate / second hand components / Parts / Assembly / Software are being used or shall be used.

We also undertake that in respect of licensed operating system/other required software, if any, the same shall be supplied along with the authorized license certificate (e.g. Product Keys, if any on Certification of Authenticity) and also that it shall be sourced from the authorized source (e.g. Authorized Microsoft Channel in case of Microsoft Operating System).

We hereby undertake to produce the certificate from our OEM supplier in support of above undertaking at the time of delivery / installation. It will be our responsibility to produce such letters from our OEM Supplier's at the time of delivery or within a reasonable time.

In case of default and we are unable to comply with above at the time of delivery or during installation, we agree to take back entire setup (i.e. Servers, Application Server Software and Backup software) for Security Solutions without demur, if already supplied and return the money if any paid to us by you in this regard.

We (system OEM name) also take full responsibility of both Parts & Service SLA as per the content even if there is any defect by our authorized Service Centre / Reseller / SI etc.

Signature of Bidder: _____

Name: _____

Business address: _____

Place:

Date:

Format 6.22

Self-Declaration for Non-Blacklisting

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

Date:

To
The General Manager
Bank of India
Head Office
Information Technology Department,
8th Floor, Star House-2, C-4, G-Block,
Bandra Kurla Complex,
Bandra East, Mumbai – 400 051

Dear Sir:

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions
Ref: Your RFP Ref: Ref: BOI:HO:IT:SS:0070 Dated: 02.05.2020

We _____ who are established and reputable hereby confirm that our company (The Auditor/ Firm/ Company/LLP) or its group company / subsidiary company / holding company /affiliate /associate company / partner should have never been black listed and/ or banned and /or barred and / or disqualified and or prohibited by SEBI and/or RBI and/or NCLT and/ or NCLAT and / or any court of law and / or quasi-judicial authority / and or any other statutory and/ or regulatory authority, in undertaking any work directly or indirectly which is required to perform as stated in this RFP and/ or issuance of any certificate of audit directly or indirectly with respect to the work sated herein the RFP”.

Yours faithfully,

Authorized Signatory (Name)

(Designation)

Note:This letter of authority should be on the letterhead of the manufacturer and should be signed by a person competent and having the power of attorney to bind the manufacturer. It should be included by the Bidder in its Bid.

Format 6.23

(to be submitted on company letter head)

**ESCALATION MATRIX of All Verticals
(To be kept in the Technical Proposal Envelope)**

**Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions
Ref: Your RFP Ref: Ref: BOI:HO:IT:SS:0070 Dated: 02.05.2020**

The escalation matrix up to top level of company is tabulated below in hierarchy-

Sr. No.	Particulars	Level-1 Escalation	Level-2 Escalation	Level-3 Escalation
1		Name: Phone No: Cell No: Email :	Name: Phone No: Cell No: Email :	Name: Phone No: Cell No: Email :

Yours faithfully,

Authorized Signatory (Name)

(Designation)

Note- Kindly mention escalation matrix of all verticals (support, sales and delivery of the company. There should be a single point of contact of senior level for verticals.

Format 6.24

Undertaking of Experience of Installation and Support of Proposed Solutions

**(This letter should be on the letterhead of both bidder and OEM separately
duly signed by an authorized signatory)**

To:
The General Manager
Bank of India
Head Office
Information Technology Department,
8th Floor, Star House-2, C-4, G-Block,
Bandra Kurla Complex,
Bandra East, Mumbai – 400 051

Sir,

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions

Ref: Your RFP Ref: Ref: BOI:HO:IT:SS:0070 Dated: 02.05.2020

We hereby undertake that we (in case of OEM) / our partner(Name of Bidder) are/is possessed expertise in implementation and support of proposed solution in compliance of RBI guidelines (and its amendments) and best industry standards.

Yours faithfully,

Signature of Authorized Signatory from OEM/ bidder _____

Name: _____

Business address: _____

Place:

Date:

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



FORMAT-6.25

**UNCONDITIONAL ACCEPTANCE OF THE TERMS & CONDITIONS OF THE RFP
(To be submitted on the bidder Company's Letter Head)**

Date:

To:
The General Manager
Bank of India
Head Office
Information Technology Department,
8th Floor, Star House-2, C-4, G-Block,
Bandra Kurla Complex,
Bandra East, Mumbai – 400 051

**Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions
Ref: Your RFP Ref: BOI:HO:IT:SS:0070 Dated: 02.05.2020**

Sir/Madam,

This is to confirm that we unconditionally accept all the terms and conditions as mentioned in the said RFP including all addendum/amendment/ corrigendum floated for Bank of India pertaining to this RFP Ref. No. **BOI:HO:IT:SS:0070 Dated: 02.05.2020**

Authorized Signatory

(Name)

Designation

Seal/Stamp of the Contractor

Date:

FORMAT-6.26

**Software/Solutions Integrity Certificate
(To be issued by OEM on OEM Company's Letter Head)**

Date:

To:
The General Manager
Bank of India
Head Office
Information Technology Department,
8th Floor, Star House-2, C-4, G-Block,
Bandra Kurla Complex,
Bandra East, Mumbai – 400 051

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions
Ref: Your RFP Ref: Ref: BOI:HO:IT:SS:0070 Dated: 02.05.2020

INTEGRITY STATEMENT

This is to certify that our product, Version:
(Hash Value -.....), developed by and a
copyright of follows standard secure coding
practices and has been tested and certified for the following checks:

- i. That the application has undergone the required level of unit, system, stress and volume tests and is free of any obvious bugs.
- ii. That the software is tested with anti-virus/anti-malware software and is free of any known virus/malwares at the time of sale.
- iii. That the application is free of any covert channels in the code being provided and subsequent modifications to be done on them.
- iv. We have evaluated the cryptographic implementation and have ensured that only cryptographic modules based on authoritative standards and reputable protocols are used.
- v. We confirm that Source code testing is carried out on application source code (to identify and detect security threats and weaknesses in its systems) and there are no OPEN vulnerabilities.
- vi. We confirm that Application Security testing is carried out for application (to identify and detect security threats and weaknesses in its systems) and there are no OPEN vulnerabilities.
- vii. We confirm that we are conducting secure coding training programs for our software developers/testers on periodical basis.

We also confirm that the above practices will be met by us for all the changes that we make in the application/ module on a regular basis.

Authorized Signatory

Date:

FORMAT-6.27

**Undertaking for Source Code and Application Security Testing
(To be issued by OEM on company's Letter Head)**

Date:

To:
The General Manager
Bank of India
Head Office
Information Technology Department,
8th Floor, Star House-2, C-4, G-Block,
Bandra Kurla Complex,
Bandra East, Mumbai – 400 051

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions
Ref: Your RFP Ref: Ref: BOI:HO:IT:SS:0070 Dated: 02.05.2020

We hereby undertake that our product has undergone following-

- i. Source code audit (Comprehensive analysis of source code for discovering bugs and security breaches and its compliance) has been done by..... (Name of Consultant).The summary on compliance /clearance of the same is attached with technical bid.
- ii. The solution has undergone SAST/DAST/IAST for application security testing and clearance /compliance of the same has been obtained from..... (Name of the firm). The same is in compliance of RBI guidelines (and its amendments) and best industry standards.
- iii. For any version change/upgrade, the solution undergone and cleared on both of above i.e. Source Code Audit and SAST/DAST/IAST for application security testing.

We also confirm that the above practices will be met by us for all the changes that we make in the application/ module on a regular basis during contract time.

Authorized Signatory (OEM)

Name-
Designation-
Place:.....
Date:

FORMAT-6.28

Project Plan

(To be submitted on the Company's Letter Head)

Date:

To:
The General Manager
Bank of India
Head Office
Information Technology Department,
8th Floor, Star House-2, C-4, G-Block,
Bandra Kurla Complex,
Bandra East, Mumbai – 400 051

Reg.: RFP for Supply, Implementation and Maintenance of IT Security Solutions

Ref: Your RFP Ref: Ref: BOI:HO:IT:SS:0070

Dated: 02.05.2020

We hereby attach the Comprehensive Project Plan (as per project management standards) along with this format in two parts-

- I. Project Management Plan
- ii. Project Implementation Plan (Solution Design, Architecture, Rollout and Installation)
- iii. Solution Support Plan post implementation

We also confirm that the above project management practices will be met by us for all the changes that we make in the application/ module on a regular basis.

Authorized Signatory

Name-

Designation-

Place:.....

Date:

**Format 6.29
CHECKLIST**

The bidder shall confirm whether following are submitted in their bid. The bidder shall indicate the page no. at which the details asked below are furnished, otherwise, bid is liable for rejection.

S.N.	DETAILS	SUBMITTED Yes/No	Page No. at which details are enclosed
1.	Technical Solutions given in Technical bid and price/rate/ cost estimate/price performance figures/cost benefit analysis etc. given in price bid only		
2.	Bids in two parts in English, sealed and super scribed (2 copies- one original and one photocopy)		
3.	Bid is filed in proper capacity files. Original and Photocopies are filed in separate files. Photocopy is complete.		
4.	Cost of RFP (non-refundable), if downloaded from the Bank's Website & Bid Security(EMD) Submitted in Qualifying & Technical BID (Part- I)		
5.	Non-disclosure agreement as per format 6.2 submitted		
6.	Manufacturers'/producers' authorization form as per format 6.8 submitted		
7.	Organizational profile as per Format 6.10 submitted		
8.	Service Support Details Form as per format 6.11 submitted		
9.	Undertaking for support services as per Format 6.14 submitted		
10.	Conformity to eligibility criteria per Format 6.16 submitted		
11.	Duly filled and signed compliance		

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



	statement in Format-6.16		
12.	Unconditional acceptance of all clauses, terms and conditions of RFP (Format clause 6.25)		
13.	Pre-contract integrity pact as per format 6.18 (Duly Signed by Authorized Signatory and Witness)		
14.	Soft Copy of Technical bid and Price bid in MSWORD /MS – Excel format		
	submitted in CD		
15.	Bids Submitted complying all parts as per Clause-3 Section B		
16.	Whether the Bid is authenticated by authorized person(Name and designation)		
17.	Address of Office on which order has to be placed		
18.	Bank and Bidder's scope, deliverable and responsibilities during warranty		
19.	All the pages are numbered properly		
20.	All pages are authenticated by sign and seal (Full signature to be affixed and not initials). Erasures/Overwriting/Cutting/Corrections authenticated Certification/Undertaking is authenticated.		
21.	The Annual Reports and Audited Balance Sheets, Company details and Capabilities submitted		
22.	Ownership certificate submitted		
23.	Details of service support and response time as per this RFP		
24.	Price bid as per the clause 3 submitted		

**Request for Proposal for Supply,
Implementation and Maintenance of IT
Security Solutions**



25.	Whether replica of price Bid is enclosed in Technical Bid masking price		
26.	Validity of the bid for one year from the date of opening of the Bid.		
27.	Support offered for 5 years on 24 hours basis on 365 day. (i.e. 24 * 7*365 basis)		
28.	Call log in Procedure, Preventive and Break down/Corrective Maintenance, Monitoring during warranty and AMC Period		
29.	Software Integrity Certificate as per format 6.26		
30.	Project Plan as per format 6.28 inline to fulfilling the Scope of the RFP		

**Request for Proposal for Supply,
Implementation and Maintenance of
IT Security Solutions**



Format 6.30

Format for Submission of Pre-Bid Queries

SR. No	RFP Page No.	RFP Clause No	RFP Clause	Clarification

Note-The bidder shall submit his queries in the above mention format strictly in excel sheet before last date of submission of pre-bid queries.

7 OTHER TERMS AND CONDITIONS (OTC)

7.1	Bid Security Amount	Rs.50,00,000/-
7.2	Bid Validity Up to	One year from the last date stipulated for receipt of responses to the Bid
7.3	Period within which Performance Security or Amendment thereto is to be submitted by the Successful Bidder upon notification of Award of Contract	30 days
7.4	Period within which the Successful Bidder should Sign the Contract after receipt of the Form of Contract.	30 days
7.5	Period of Performance Contract (from the Date of Award of Contract)	Minimum 5 years
7.5	Performance Security Amount	10% of Amount of contract value for 5 year period
7.6	Warranty support period for every Solution	12 months from date of user acceptance
7.7	User Acceptance tests	Refer : Clause 4.7
7.8	Period within which Supplier to remedy defects after having been notified of the same	Maximum 4 hours