Bank of Maharashtra

(One Family… One Bank… Mahabank)

Request for Proposal for Supply, Installation & Maintenance of Security Solutions (Data Loss Prevention (DLP), Data Identification & Classification Tool (DICT), Database Activity Monitoring (DAM), Endpoint Encryption (EE) & Patch Management Solution (PMS))

TENDER REFERENCE # RFP - 082020

बैंक ऑफ महाराष्ट्र
Bank of Maharashtra
ONE FAMILY ONE BANK

Head Office, 'LOKMANGAL'
1501, Shivaji Nagar, Pune – 411 005

Cost of Tender Document: INR 29,500/-

Contents

Important Clarifications:

Following terms are used in the document interchangeably to mean:

1. Bank means 'Bank of Maharashtra '
2. Bidder/SI/Vendor means the respondent to the RFP document.
3. RFP means the Request for Proposal document
4. DC means Bank's Primary Data Canter, DR / DRC/ DRS means Bank's Secondary/Disaster Recovery Site. NS means Bank's Near Site hosting infrastructure for Zero data loss.
5. Bidder and Bank shall be individually referred to as 'Party' and collectively as 'Parties'.
6. Bidder / Respondent – signifies those who purchase this tender document and submits response to it.

This document is meant for the specific use by the Company / person/s interested to participate in the current tendering process. This document in its entirety is subject to Copyright Laws. The bidders or any person acting on behalf of the bidders should strictly adhere to the instructions given in the document and maintain confidentiality of information. The bidders will be held responsible for any misuse of information contained in the document, and liable to be prosecuted by the bank in the event that such a circumstance is brought to the notice of the bank. By downloading the document, the interested party is subject to confidentiality clauses.

List of Abbreviations

Acronym	Full Form
AD	Active Directory
ADS	Active Directory Services
AM	Approach and Methodology
AMC	Annual Maintenance Contract
ATS	Annual Technical Support
BC	Business continuity
BFSI	Banking, Financial Services and Insurance
BOM	Bill of Materials
BRS	Business Requirement Specification
CB	Commercial Bid
CBS	Core Banking Solution
CCN	Credit Card Number
CCPA	California Consumer Privacy Act
CD	Compact Disk
CDM	Cash Deposit Money
CIFS	Common Internet File System
DAM	Database Activity Monitoring
DB	Database
DBMS	Database Management System
DC	Data Centre
DICT	Data Identification & Classification Tool
DLP	Data Loss Prevention
DR	Disaster Recovery
DVD	Digital Versatile Disc
EE	Endpoint Encryption
EMD	Earnest Money Deposit
FM	Facility Management
FR	Functional Requirements
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
HA	High Availability
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IM	Instant Messaging
IRM	Information Rights Management
IS	Information Security

Acronym	Full Form
ISMS	Information Security Management System
ISO	International Standards Organisation
IT	Information Technology
ITAM	IT Asset Management
ITSM	IT Service Management
LDAP	Lightweight Directory Access Protocol
LPT	Line Print Terminal
MS SQL	Microsoft structured query language
MTA	Mail Transfer Agent
MTP	Media Transfer Protocol
NOC	Network Operations Centre
OCR	Optical Character Recognition
OEM	Original Equipment Manufacturer
OS	Operating System
P2P	Peer to Peer
PAN	Permanent Account Number
PB	Project Demonstration & Bid Presentation
PBG	Performance Bank Guarantee
PCI	Payment Card Industry
PII	Personally identifiable information
PIM	Privileged Identity Management
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PMS	Patch Management Solution
PO	Purchase Order
PoP	Point of Presence
PSB	Public Sector Banks
PSU	Public Sector Undertaking
RBAC	Role Based Access Control
RBI	Reserve Bank of India
RCA	Root cause analysis
RDBMS	Relational Database Management System
RDP	Remote Desktop Protocol
RFP	Request for Proposal
RPO	Recovery point objective
RRB	Regional Rural Banks
RTO	Recovery Time objective
SAN	Storage Area Network
SCB	Scheduled Commercial Bank

Acronym	Full Form
SD	Secure Digital
SFTP	Secure File Transfer Protocol
SI	System Integrator
SIEM	Security Information & Event management
SLA	Service Level Agreement
SME	Small and Medium Enterprises
SMTP	Simple Mail Transfer Protocol
SOP	Standard Operating Procedures
SSH	Secure Shell
SSL	Secure Sockets Layer
SSN	Social Security Number
STIG	Security Technical Implementation Guides
T&D	Training and Development
TACACS	Terminal Access Controller Access-Control System
TB	Technical Bid
TCO	Total Cost of Ownership
TLS	Transport Layer Security
TR	Technical Requirements
UAT	User acceptance Testing
UI	User Interface
UID	Unique Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
VA	Vulnerability Assessment
WPD	Windows Portable Devices

1. Invitation to the Tender

This is to inform that Bank of Maharashtra (BoM) invites sealed tenders for Technical bid and Commercial bid from eligible bidders for supply, installation, commissioning and maintenance of Data Loss Prevention (DLP), Data Identification & Classification Tool (DICT), Database Activity Monitoring (DAM), Endpoint Encryption (EE) & Patch Management Solution (PMS) as On-premises security solutions.

The bidders are expected to examine all instructions, forms, terms, BoM project requirements and other information in the RFP documents. Failure to furnish all information required as per the RFP document or submission of a proposal not substantially responsive to the RFP document in every respect will be at the Bidder's risk and may result in rejection of its Proposal and forfeiture of the Bid Earnest Money Deposit.

A complete set of tender documents may be purchased by eligible bidder upon payment of a non-refundable fee, mentioned in the important information regarding bid submission, by demand draft / banker’s cheque in favour of Bank of Maharashtra and payable at Pune.

This tender document is not transferable. Only the bidder, who purchased this tender is entitled to quote.

Important information regarding Bid submission

Tender Reference # RFP - 082020	
Price of Tender copy	Rs.25,000/- + Rs.4,500/- (GST) = Rs.29,500/-
Date of commencement of issue of tender document	07.09.2020
Date of closure of tender document	21.10.2020 up to 14:00 hrs.
Bid Security Deposit (EMD)	Rs.50,00,000/- (Fifty Lakhs Only)
Queries to be mailed by	18.09.2020 up to 17:00 hrs.
Queries to be mailed to	agmdc@mahabank.co.in dccm@mahabank.co.in rajkiran.lalam@mahabank.co.in prashant.chavan@mahabank.co.in jeyasakthi.somasundaram@mahabank.co.in
Pre Bid Meeting	25.09.2020 at 11:30 hrs.
Last Date and Time for receipt of tender offers	21.10.2020 up to 14:00 hrs.
Date of opening of technical bids	21.10.2020 at 16:00 hrs.
Date of opening of commercial bids	Will be informed to Technically qualified bidders separately
Address of Communication	Deputy General Manager Information Technology Bank of Maharashtra, Head Office, “Lokmangal” 1501, Shivajinagar, Pune – 411 005.
Contact Telephone Numbers	***(020) 27335324/ 5314***
E-mail Id	agmdc@mahabank.co.in dccm@mahabank.co.in rajkiran.lalam@mahabank.co.in prashant.chavan@mahabank.co.in jeyasakthi.somasundaram@mahabank.co.in
Website	https://www.bankofmaharashtra.in

The copy of RFP document may be obtained during office hours on aforesaid working days in person by paying an amount of **INR 29,500/- (Non-refundable) inclusive of GST** by way of Demand Draft / Pay Order favouring “BANK OF MAHARASHTRA” payable at Pune. Bank reserves the right to reject any or all offers without assigning any reason.

Please note that the prospective bidder needs to purchase the tender document from Bank and is invited to attend the pre-bid meeting on above date and time at Bank of Maharashtra, Head Office, Pune. In case the prospective bidder downloads the document from website of the Bank, the cost of tender document should be paid along with the Bid response. However, in order to participate in the pre-bid meeting, that tender document must be purchased by the prospective bidder.

Earnest Money Deposit must accompany all tender offers as specified in this tender document. EMD amount/Bank Guarantee in lieu of the same should not be mixed with Technical / Commercial bid. It should be in separate cover to be handed over to the department.

Tender offers will be opened in the presence of the bidder representatives who choose to attend the opening of tender on the above-specified date, time and place.

Technical requirements, Terms and Conditions and various formats and pro-forma for submitting the tender offer are described in the tender document.

General Manager
Information Technology

2. Introduction

2.1 About the Bank

Bank of Maharashtra is a public sector bank with a standing of more than 84 years. It has a three tier organizational set up consisting of branches, Zonal Offices and Head Office. Bank of Maharashtra, a leading Public Sector Bank has more than 1874 fully computerized branches spread across the country. In the state of Maharashtra itself, it has about 1130 branches, the largest network of branches by any Public Sector Bank in the state. The Bank has set up specialized branch offices to cater to the needs of SMEs, Corporate, agriculturists and importers & exporters.

The Bank has fine-tuned its services to cater to the needs of various sections of society and incorporated the latest technology in banking offering a variety of services. The products and services offered by the Bank includes demand deposits, time deposits, working capital finance, term lending, trade finance, retail loans, government business, Bancassurance business, mutual funds and other services like demat, lockers and merchant banking etc.

This request for proposal document (‘RFP document’ or RFP) has been prepared solely for the purpose of enabling Bank of Maharashtra (‘Bank’) to select a Bidder for supply, install, configure and provide onsite comprehensive warranty & AMC/ATS services for the period of contract. The RFP document is not recommendation, offer or invitation to enter into a contract, agreement or any other arrangement, in respect of the services. The provision of the services is subject to observance of selection process and appropriate documentation being agreed between the bank and any successful bidder as identified by the bank, after completion of the selection process as detailed in this document.

2.2 Project Objective

The Bank envisages selecting a Bidder who will provide end to end Information Security Solution products and services such as (and not limited to) design, size, procure, supply, implement, maintain, manage, handhold and provide subsequent facilities management, comprehensive onsite warranty/AMC/ATS in the following areas:

a) Data Loss Prevention (DLP)
b) Data Identification & Classification Tool (DICT)
c) Database Activity Monitoring (DAM)
d) Endpoint Encryption (EE)
e) Patch Management solution (PMS)

The above list of applications would be considered as ‘Security Solutions’ in this RFP. This will be inclusive of hardware and all related software and services required for the proper functioning of the solutions. The bidder shall include all the products & services as per the RFP requirement in Annexure 10 - Commercial Bill of Materials and deliver the same to the Bank’s location while adhering and synchronizing the delivery schedule to meet the implementation timelines mentioned in Clause 2.3.1.

2.3 Project Scope in brief

A. The Bidder’s scope is defined in this **Request for Proposal** document which encompasses the Annexures & Appendices and subsequent Addenda & Corrigenda (hereinafter referred to as “**RFP**” or “**Tender**”). This is for the Bank’s Domestic Operations.
B. The contract tenure will be for **FIVE Years** from the Date of Acceptance of the Solutions by the Bank.

C. Bank has already implemented DLP, DAM, EE & PMS Solutions from various OEMs and the product deployment details will be shared with the successful Bidder. Bidder has to arrange for migrating the existing policies/rules to the Solution provided by the Bidder.

D. Bidder shall maintain business continuity, as per agreed business continuity plan.

E. Bank will provide necessary Hardware/System Infrastructure for UAT/Development/production environment, OS, Storage, Server in VM, Racks, required network components & connectivity. Bank has ORACLE ULA in place, however the bidder may also propose solution that uses different database, price of the same shall be included by the bidder in their commercials as per the format. Bidder must quote the price for the same in their commercials as per the format. The successful bidder shall implement the proposed solutions based on the same and take care of installation, configuration, support and its further maintenance.

F. Bidder must maintain all involved application/database level components required for the proposed solution. In case, if Bidder is supplying the customised OS, then the Bidder has to take care of OS level installation, configuration, support and its further maintenance as well.

G. If Bidder is supplying appliances or any other hardware for specific solution components which cannot be hosted at VM level, Bidder must quote the price for the same under hardware cost in their commercials as per the format.

H. This RFP has been prepared solely to enable Bank of Maharashtra (hereinafter referred to as “Bank” or “BOM”) to appoint a suitable Bidder for supplying, designing, procuring, installation, commissioning, customization, testing, implementing, integration and maintaining/maintenance of the end to end applications/Solutions as listed below:

a) Data Loss Prevention (DLP)
b) Data Identification & Classification Tool (DICT)
c) Database Activity Monitoring (DAM)
d) Endpoint Encryption (EE)
e) Patch Management Solution (PMS)

The above stated applications are hereby referred to as security solutions.

The Bidder is required to deploy the above solutions adequately sized and scalable Hardware, Software, Applications, Tools, Utilities, related Services and Facilities Management as per Specifications, terms and conditions and scope defined in this RFP (hereinafter referred as “Security Solution”).

A. Rollout the proposed solutions covering all the Bank’s locations as specified under the scope.
B. Migrate Rules/Policies from existing DLP, DAM, EE & PMS Solutions to the Solution proposed by the Bidder
C. Impart Training and Knowledge Management to the Bank’s management and personnel.
D. Provide Facilities Management Services for the implemented solutions.
E. Provide complete hand-over along with detailed documentation on at the end / termination of the contract period.

2.3.1 Project Schedule

Stage	Activity	# Weeks	Project Duration(in weeks)	Time Period for completion
1	Submission of Detailed Project Plan including integrating all the present security solutions	2	2	2 weeks from issue of Purchase Order
2	Deployment of Resources at Bank's premises for Solution Proposed	4	4	4 Weeks of issuing the Purchase order to SI
3	Pre Implementation Training to bank staff	1	4	4 Weeks of issuing the Purchase order to SI
4	Delivery of related Hardware/Software, licenses and deployment of resources at bank premises	1	5	5 weeks from issue of Purchase Order
5	Installation and Configuration of Hardware/Applications in DC & DR	2	7	7 weeks from issue of Purchase Order
6	Integration of Installed security solution with other applicable deployed solution in Bank Environment	3	10	10 weeks from issue of Purchase Order
7	UAT (functional testing) of Deployed Security Solutions	2	12	12 weeks from deployment of resources
8	Implementation of complete solution as per RFP scope in all locations. Impact analysis after implementation of the solutions need to be examined. To simplify the analysis, bidder can plan to implement one solution at a time. After successful implementation of one solution, next solution can be implemented.	6	18	18 weeks from deployment of resources
9	Post Implementation Training	1		Within 6 month from Date of Project Implementation

Pert Chart:

Description	W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15	W16	W17	W18
Submission of Detailed Project Plan including integrating all the present security solutions	■	■																
Deployment of Resources at Bank's premises for Solution Proposed	■	■	■	■														
Pre Implementation Training to bank staff	■	■	■	■														
Delivery of related Hardware/Software and license and deployment of resources at bank premises	■	■	■	■	■													
Installation and Configuration of security Hardware/Applications in DC & DR	■	■	■	■	■	■	■											
Integration of Installed security solution with other applicable deployed solution in Bank Environment	■	■	■	■	■	■	■	■	■	■								
UAT (functional testing) of Deployed Security Solution	■	■	■	■	■	■	■	■	■	■	■	■						
Implementation of complete solution as per RFP scope in all location)	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

2.3.3 Training

Selected bidder shall provide the training to the bank's personnel as described below:

i. The training should include the architecture, hardware, software, integration, and customization, policy installation, troubleshooting, reporting and other aspects of the solution.

ii. This faculty should be solution certified up to advance level and should provide courseware with adequate lab facility as well. The training should be provided by the OEM employee and should be of minimum 3 days, 8 hours a day for each solution under this RFP. Training should be provided to number of personnel identified by Bank on functional, operational and reporting aspects of the entire security solution. Pre implementation training must be provided before project implementation and post implementation training must be provided after successful implementation. At the end of training participants shall be given certificate of successful completion by the OEM.

iii. Bidder should arrange refresher training on deployed solution in subsequent year of project tenure. Refresher training should cover the Feature/Functional advancement in deployed solution.

iv. Bidder should submit detailed course content and provisional agenda along with the Bid.

2.4 Schedule of Events

For Schedule of events; refer to table under the clause “Invitation to tenders” on page no. 10 of this RFP.
# All queries / requests for clarification from Bidders must reach us by e-mail or in person before the timelines mentioned in clause “Invitation to tenders”. Shall the Bidder have any queries or require any clarification, Bidder shall request the clarification from the Bank for Terms & conditions related queries / clarifications and in “Annexure 8 – Pre Bid Query Format” for technical or other non – Terms & condition related queries / clarification. No clarification or queries will be responded in any other format. The Bidder shall make sure that all the queries and clarifications reach Bank before the timelines mentioned in clause “Invitation to tenders”.

The Bank reserves the exclusive right to make any amendments / changes to or cancel any of the above actions or any other action related to this RFP.

The Bidder is required to provide a detailed strategy to the Bank; the activities mentioned above are indicative but the timelines for procurement and delivery shall be maintained. Hence, if the Bidder has a quicker and effective solution the same may be discussed and agreed by the Bank.

3. RFP Response terms

3.1 Lodgment of RFP Response

Tender Fee

The non-refundable tender fee, as mentioned in Clause 1 of this RFP, shall be paid by way of Bankers Cheque / Demand Draft / Pay Order favouring Bank of Maharashtra, Payable in Pune, which is non-refundable and must be submitted separately along with RFP response.

RFP Closing Date

RFP Response should be received by the officials indicated not later than the date and time mentioned in Clause 1 of this RFP.

Late RFP Policy

RFP responses received after the deadline for lodgement of RFPs at the address mentioned will not be accepted by Bank and hence the bidders are advised to submit their responses within the time and no excuses / reasons for delay will be accepted by Bank.

RFP Validity Period

RFP responses will remain valid and open for evaluation according to their terms for a period of at least six (6) months from the RFP closing date. Bank / its subsidiaries shall have the right, at its sole and absolute discretion, to continue the assignment / contract on the selected bidder for future requirement on the rates finalized in this processing for various items / activities as described in the Price Bid after expiry of current assignment period.

3.2 Requests for Information

The bidders are required to direct all communications for any clarification related to this RFP, to Bank officials as mentioned in Clause 1 of this document and in writing. All queries relating to the RFP, technical or otherwise, must be in writing only. Bank will try to reply, without any obligation in respect thereof, every reasonable query raised by the Recipients in the manner specified. However, Bank will not answer any communication initiated by respondents later than five business days prior to the due date for lodgement of RFP response. Bank may in its absolute discretion seek, but under no obligation to seek, additional information or material from any Respondents after the RFP closes and all such information and material provided must be taken to form part of that Respondent's response. Respondents should invariably provide details of their email address as responses to queries will only be provided to the Respondent via email. If Bank, in its sole and absolute discretion, deems that the originator of the query will gain an advantage by a response to a question, then Bank reserves the right to communicate such response to all Respondents. Bank may, in its sole and absolute discretion, engage in discussion or negotiation with any Respondent (or simultaneously with more than one Respondent) after the RFP closes to improve or clarify any response.

3.3 Notification

Bank will notify the Respondents in writing as soon as practicable, but not later than 10 working days from the RFP evaluation completion date, about the outcome of the RFP evaluation process, including whether the Respondent's RFP response has been accepted or rejected. Bank is not obliged to provide any reasons for any such acceptance or rejection.

3.4 Disqualification

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

3.5 Timeframe

The timeframe for the overall selection process will be as mentioned in this RFP in Clause 1:"Invitation to the Tender"

Bank reserves the right to vary this timeframe, at its absolute and sole discretion, and without providing any notice/intimation or reasons thereof. Changes to the timeframe will be relayed to the affected Respondents during the process.

The time schedule will be strictly followed. Interested parties should adhere to these timelines. However, Bank reserves the right to change the aforementioned timelines.

3.6 Integrity Pact

To ensure transparency, equity, and competitiveness and in compliance with the CVC guidelines, this tender shall be covered under the Integrity Pact (IP) policy of Bank. The pact essentially envisages an agreement between the prospective bidders/vendors and Bank committing the persons/officials of both the parties, not to exercise any corrupt influence on any aspect of the contract. The format of the agreement is enclosed in Annexure 13.

Signing of the IP with Bank would be one of the preliminary qualification for further evaluation. In other words, entering into this pact would be one of the preliminary qualification for this tender and the pact shall be effective from the stage of invitation of bids till the complete execution of the contract. Foreign Bidders shall disclose the name and address of agents and representatives in India and Indian Bidders shall disclose their foreign principles or associates. Any vendor/bidder not signed the document or refusing to sign shall be disqualified in the bidding process.

Bidders shall disclose the payments to be made by them to agents/brokers or any other intermediary. Bidders to disclose any transgressions with any other company that may impinge on the anti-corruption principle.

The Integrity Pact envisages a panel of Independent External Monitors (IEMs) to review independently and objectively, whether and to what extent parties have complied with their obligation under the pact. The IEM has the right to access to all the project document.

The name and contact details of the Independent External Monitors (IEM) nominated by Bank are as under:

Shri. Nilmoni Bhakta Address - A-801, PBCL CHS Ltd., Plot No. 3, Sector 46 A, Nerul, Navi Mumbai, 400706 Email - nilmoni.bhakta@gmail.com	Shri. Madan Lal Sharma Address - K-23, Jangpura Extention New Delhi Email - ml.sharma1965@yahoo.com

Bank at its sole discretion reserves the right to change/name another IEM, which shall be notified latter.

Same terms (including payment terms) which were applicable during the term of the contract should be applicable for reverse transition services.

The bidder agrees that after completion of the Term or upon earlier termination of the assignment the bidder shall, if required by Bank, continue to provide facility to Bank at no less favourable terms than those contained in this tender document. Unless mutually agreed, the rates shall remain firm.

Bank shall make such prorated payment for services rendered by the bidder and accepted by Bank at the sole discretion of Bank in the event of termination, provided that the bidder is in compliance with its obligations till such date. However, no payment for “costs incurred, or irrevocably committed to, up to the effective date of such termination” will be admissible. There shall be no termination compensation payable to the bidder.

Termination shall not absolve the liability of Bank to make payments of undisputed amounts to the bidder for services rendered till the effective date of termination. Termination shall be without prejudice to any other rights or remedies a party may be entitled to hereunder or at law and shall not affect any accrued rights or liabilities or either party nor the coming into force or continuation in force of any provision hereof which is expressly intended to come into force or continue in force on or after such termination.

3.7 Amalgamation

If the Bank undergoes an amalgamation, take-over, consolidation, reconstruction, merger, change of ownership etc., this RFP shall be considered to be assigned to the new entity and such an act shall not affect the rights and obligations of the Vendor under this RFP.

3.8 Annexure Seeking Response for Evaluation

A detailed set of annexure is provided to the bidder for formulation of responses. These annexure would assist Bank in effectively normalizing the bidder's response for various areas including bidder's qualification criteria, technical requirements, commercial proposals etc. The list of such annexure is provided in the table below:

Annexure Number	Name of the Annexure
Annexure 1	Technical and Functional Requirements
Annexure 2	Technical Bid Format
Annexure 3	Conformity with Hardcopy Letter
Annexure 4	Conformity Letter
Annexure 5	Eligibility Criteria Compliance
Annexure 6	Cover Letter
Annexure 7	Application Management Services
Annexure 8	Pre-bid Query Format
Annexure 9	Bid Security Form
Annexure 10	Commercial Bill of Material
Annexure 11	Compliance Statement for Reverse Auction
Annexure 12	List of Deviations Requested
Annexure 13	Pre-Contract Integrity Pact
Annexure 14	Manufacturer's Authorization Form
Annexure 15	Resource Deployment Plan
Annexure 16	Guidelines, Terms & Conditions and Process Flow for E-Procurement Auction
Annexure 17	Past Experience
Annexure 18	List of Reports
Annexure 19	Performance Bank Guarantee
Annexure 20	Authorization Letter
Annexure 21	Non-Disclosure Agreement
Annexure 22	Resource plan matrix
Annexure 23	Undertaking of Information Security
Annexure 24	List of Supported devices by OEM
Annexure 25	End Of Sale/End of Life/ End of Life Information

4. Detailed Scope of work

4.1 Overview

The Bank's business objectives in striving to offer innovative products and superior service. Bank further desires to strengthen its Information Security setup by implementing the following security solutions, which shall complement the Bank's existing network & security deployment:

a) Data Loss Prevention (DLP)
b) Data Identification & Classification Tool (DICT)
c) Database Activity Monitoring (DAM)
d) Endpoint Encryption (EE)
e) Patch Management Solution (PMS)

Bank is already using DLP, DAM, EE & PMS Solutions from various OEMs and the product deployment details will be shared with the successful Bidder. Bidder has to arrange for migrating the existing policies/rules to the bidder proposed solution.

Common Scope of Work for Proposed Solutions

4.1.1 The Bank's Data Centre, Near site & Disaster Recovery Site details will be shared with the successful Bidder.

4.1.2 The bidders are expected to consider the current deployment & propose the solutions which Integrate with the existing solutions and ensure that all the proposed new solutions would complement well with the Bank's existing network & security setup. In case the bank revamps its current architecture or completely migrates to another network technology/New location due to any reason, the bidder shall make necessary changes in its solution to adapt to new deployment without any additional cost to the Bank.

4.1.3 The Bidder is required to supply the Software/Hardware/Licenses/Applications required to provide above solutions at DC, DRC, NS & Branches and other Bank locations PAN India, as applicable. The solutions shall comply with the technical requirement provided in Annexure 1 – Technical & Functional requirements.

4.1.4 The Bidder must ensure that quoted Software and Hardware should not be end of sale within 5years of supply to the Bank. Bidder shall also ensure that no component is declared either End of Support, End of Life during tenure of the contract. In case the bidder/ OEM fails to give the above data for any specific component, and later on, any specific component is found to have date of end of sale/ support/ life which falls before the end date of the contract the bidder will have to replace / upgrade the component free of cost with the latest workable component. Bidder is required to submit the declaration from the OEM to that effect.

4.1.5 In case the bidder fails to replace/ upgrade the component within 3 months from the date of declaration by OEM (even when the Bank notices it later) then that will be considered as breach of contract and the bidder will be liable to legal prosecution including termination of the contract. Additionally, till the time the component is replaced, the bidder shall be liable for penalty as per SLA clause from the date of declaration by OEM

4.1.6 The delivery plan must be synchronized with the project delivery timelines of the Bank. (Clause 2.3.1 of this document) Bidder is required to make available required resources that may be required for the successful completion of the entire assignment within the quoted cost to the Bank. Furthermore, the delivery shall be year over year as indicated in the Bill of material.

4.1.7 All the Software shall come with 1-year onsite comprehensive warranty subsequently Facilities Management and Warranty/AMC/ATS support for the additional 4 years. The Hardware shall come with 3 years onsite comprehensive warranty subsequently the Bidder shall provide the facilities management and Warranty/AMC/ATS support for the additional 2 years.

4.1.8 Solution should be consisting of hardware, software, operating system, database, online / offline storage, analytical applications and tools, etc. as per the technical and operational specifications of the Bank. Refer Technical Specification of Solutions.

4.1.9 The Bank would also like the bidders to demonstrate their solution capabilities, integration services and any other innovative and creative services, which the bidder can offer to supplement bank's requirements during the RFP technical evaluation & presentation process.

4.1.10 Bank reserves the right to bring about any changes in Requirement/Scope of this RFP and the same will be communicated to the bidder well in time so as to allow the bidder to prepare their proposal.

4.1.11 The solution must integrate with various systems / applications in the Bank including but not limited to SIEM, PIM, NOC, TACACS, ITAM, ADS and ITSM etc.

4.1.12 All the licenses shall be in subscription based. There should not be any limitation on the number of applications and users using the solution. Other specific condition may be refer from technical document attached as Annexure-1

4.1.13 OEM/SI (System Integrator) has to arrange for the prompt, conclusive, secure and permanent closure of any vulnerability pointed out in any of the security Review or Audits carried by the bank or bank appointed third party.

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

- Procurement of the necessary solutions and the corresponding hardware, software, database etc. required for implementing these solutions at the bank.
- Implementation of the identified solutions at Bank including configuration, customization & Integration of the products as per the requirement. Also, implemented solution must meet bank's system security requirements.
- Bidder to specify the need of VM or other hardware for storage or hosting of application in their technical bid.
- The bidder shall provide the detailed technical architecture comprising of hardware (including configuration) with operating systems and other application software in their technical bid.
- In case the bidder has not indicated any peripherals /equipment in their proposed solution and if same is required for successful implementation of proposed solution then cost of those components should be borne by the bidder.
- Bidder shall apply all software updates / version upgrades released by the respective OEMs during the contract period .

4.1.15 Central device should store minimum 6-month access/application logs on internal storage**.**

4.1.16 The bidder may propose any architecture at the time of technical bid submission, which is cost effective, takes care of high availability and also redundancy, in case DC fails and during DR drill as well.

4.1.17 All hardware/software offered is required to be on-premises licensed to Bank of Maharashtra. Bidder is required to size all the hardware/software for the solution proposed. During the warranty period of the appliance/hardware or software, in case of any shortfall of software licenses or Hardware sized; bidder is required to provide software / hardware at no additional cost to Bank of Maharashtra.

4.1.18 The solutions and services in scope should be designed with adequate redundancy and fault tolerance to ensure compliance with SLAs for uptime as outlined in this RFP. Bidder should design the solution in line with best industry practices.

4.1.19 Bidder shall also undertake to carry out implementation / operationalization including move, add and delete, changes / customization of such hardware & software updates, releases, version upgrades. Implemented solution must meet Bank of Maharashtra system security requirements.

4.1.20 Bidder shall migrate the rules/policies configured in existing DLP, DAM, EE & PMS Solutions to the solution proposed by the bidder. If migration is not possible, Bidder has to configure the same rules/policies in the proposed solution and ensure similar outcome in line with the existing solution. Bidder can also fine-tune such policies/rules in case if requires.

4.1.21 The overview of the envisaged deployment & the coverage of the proposed solutions is depicted in below table:

S. No	**Solution**	**Centralised monitoring & management (infrastructure requirement) #**		**Coverage**				
		DC	**DR**	**DC**	**DR**	**HO**	**Branches**	**Other Bank Locations**
1	DLP	Y	Y	Y	Y	Y	Y	Y
2	DICT	Y	Y	Y	Y	Y	Y	Y
3	DAM	Y	Y	Y	Y	Y	N	N
4	EE	Y	Y	Y	Y	Y	Y	Y
5	PMS	Y	Y	Y	Y	Y	Y	Y

(#) – The infrastructure & applications required for centralized monitoring & management of the proposed solutions (for e.g Servers / appliances as the part of the proposed solution along with respective s/w & database) will have to be deployed in the Bank's DC and DRC (as depicted above).The Bank would prefer to have all the hardware/appliance infrastructure within the DC/DRC however if the Bidder's solution necessities the deployment of a hardware/applications outside any of these locations then the Bidder must highlight the same in their architecture and factor that in the Bill of materials well.

POC (Proof of Concept):

Technically qualified bidders should conduct POC (Proof of Concept) within 1 week (7 Working days from the date of mail sent to the technically qualified bidders) as per the above mentioned scope of work and as per the technical requirements and technical Specifications on the Bank's Network. Performance and impact analysis will also be tested as a part of POC. After successful completion of the POC (Proof of Concept), the commercial bids will be opened only for the technically qualified bidders. The Bank may reject the technically qualified bidder/s, if the solution provided is not technically feasible and does not meet the scope of work, technical requirements & technical specifications during the POC (Proof of Concept). Bank will decide the duration of POC depends upon the count of technically qualified bidders and the proposed OEMs.

4.2 Data Loss Prevention (DLP)

Bank intends to implement Data Loss Prevention solution covering the endpoints located at all locations of the Bank to prevent the loss of confidential Bank data / Bank customer information that could leak out of the Bank and would enable bank to reduce the corporate risk of the unintentional or intentional disclosure of confidential information. The solution shall also include capability to control changes to critical documents thus ensuring sanctity of data. This can be termed as data control for both DLP and Compliance. The management and monitoring of DLP solution to be done from Centralized location at DC and DRC. The solution shall have adequate redundancy built in.

4.2.1 The Bidder is required to design & size the Data Loss Prevention (DLP) solution at DC and DRC. Currently Bank has about 15000 endpoints including desktops, servers & laptops. The Bank envisages the increase in the number of end points to 25000 during the tenure of 5 years. The bidders proposed solution shall be sized to meet the 5 year requirement. However, the solution shall be scalable to cover 30000 endpoints. The Bidder is also required to install, configure & provide comprehensive onsite warranty & AMC/ATS services and facilities management for the same over the tenure of the contract.

4.2.2 The Bidder is expected to provide Data Leakage Prevention solution, covering but not limited to:

a) End point

b) Email

c) HTTP/S and FTP

d) Integration with SIEM

e) Analytics

f) Perform Data discovery

g) Scanned Documents

4.2.3 The proposed DLP solution shall consist of following broad functionalities:

a) Discover Sensitive data

b) Monitor user actions to understand the risk involved

c) Educate the users and the management so as to reduce the risk.

d) Enforce security controls

4.2.4 The proposed DLP solution shall have the minimum following features:

4.2.4.1 Identify data leakage across all vectors, irrespective of policy being in place or not

4.2.4.2 Protect data

4.2.4.3 Have flexible control over Remediation of Data Leakage

4.2.4.4 Ease of Use and Quick to Deploy

4.2.5 The Functional requirements of the Bank with respect to the Data Loss Prevention solution are as follows:

a) Proposed Data Loss Prevention Solution shall be able to have controls that encompass the entire Corporate Network of Bank. It shall encompass Network, storages and endpoints as well. The solution shall be able to start at the very basic level and progress to subsequent advanced levels of usage. The solution shall be device agnostic. The bidder shall involve its best resources for development of policies that takes risk based approach.

b) Data protection shall also involve being able to identify known and unknown plug and play devices being connected to critical data resources. Also, the solution shall seamlessly integrate with Encryption which shall be intelligent enough to enforce Encryption of sensitive data.

c) The DLP solution shall be able to go beyond known policies and provide Forensic capability on all historic data. Thus, the DLP shall safeguard sensitive data and ensure compliance by protecting sensitive data wherever it lives on the network or in storage systems, while saving time and money with centralized deployment, management, and reporting.

d) Quick Deployment capability and Single Management Console for configuring Uniform Policies across Network

e) Capability to Monitor all traffic flowing out of the Network, irrespective of Policies being in place or not

f) Ability to handle data being written over different types of Media and option to Monitor or Prevent the same

g) Ability to seamlessly integrate with Encryption and selectively Encrypt data on the basis of designed policies

h) Enforce Compliance over data sitting in different locations and be able to Remediate

i) Employ different fingerprinting methods to signify sensitive data

j) Be Protocol and Port agnostic so as to tackle non-standard Data Transfer channels

k) Forensic Capability of searching through all the past traffic

l) Capability to exert sufficient control on external devices being connected in the environment

m) Flexible Reporting options for technical as well as High level reports

n) Proposed DLP & DICT solution should be fully compatible with each other and should have proven records on seamless & effective integration and further utilization

4.2.6 Multiple Deployment options comprising of Hardware and Software. The Bidder is required to monitor all relevant data leaving the Network and be able to create policy for protection and implement the same.

4.2.7 The Bidder is required to locate all of the Sensitive data and classify it according to set process. The bank or its appointed consultant will classify the data based on criticality. The bidder shall also ensure that any new data format or data types flowing over network is detected and is included in the rule set within 24 hours of detection of data.

4.2.8 The Bidder is required to put in place prevention or protection rules for that data deemed necessary.

4.2.9 The Bidder is required to install the data control for identifying any change in the critical files identified by the bank.

4.2.10 The Bidder shall configure integrity monitoring for the files and ensure write protection wherever necessary.

4.2.11 There shall be adequate audit trail capability to identify drift in the document and all the relevant details like who made what changes and change details.

4.2.12 Audit shall allow for Reporting and Search capabilities.

4.2.13 The Bidder shall provide the training of the deployed solution to the Bank personnel for 1 batch with 8 persons.

4.2.14 The Bidder shall involve their resources in Data Collection, Policy/Rule Creation/Fine-Tuning, Policy/Rule Enforcement and Incident Management Support.

4.2.15 The Bidder shall be abide by the Incident/Alert Closure timeline defined by the Bank according to alert/incident severity and co-ordinate with Data/Policy Owners to ensure closure of incidents within the stipulated timeline.

4.2.16 Bidder shall conduct awareness programs among end users as and when Bank requires.

4.2.17 The DLP Solution shall duly meet the minimum technical requirements as specified in Annexure 1 – Minimum Technical requirement. The Bidder shall ensure that the bill of material is in compliance to the technical requirements

4.3 Data Identification & Classification Tool (DICT)

Bank intends to implement Data Classification Tools for approximately 15,000 users and Data Identification Tool to Search and classify the critical Data at rest automatically as per defined criteria in shared folder and bank specified data repositories. As of now, Bank envisages the Data at Rest which is about to classify for next 5 years would be around 100TB approximately. Bidder has to quote by considering the above parameters and supply the additional user/data wise licenses in the same cost during the tenure of Contract if Banks requires.

4.3.1 Solution should improve Data Loss Prevention Accuracy and should offer seamless integration with proposed DLP Solution. Proposed DLP solution should leverage the use of this tool.

4.3.2 Solution should provide visibility of critical data in the Bank.

4.3.3 Solution should raise security awareness among end users and educate them on data handling.

4.3.4 Proposed Solution should enable to establish a policy-driven foundation that helps to identify and classify sensitive data at creation, in motion, or at rest and apply the right security policy to protect it. Solution should work with email and office applications as a part of user's day-to-day workflow for identification and classification of mails and documents.

4.3.5 Policy engine of proposed solution should provide granular options to build policies based on various conditions like AD user, department, file content, file attributes, recipients, location, printer, etc., and these policies shall be triggered based on different Events like creating a new file, opening an existing file or emailing a document, etc.

4.3.6 Solution should classify other file/file types on Windows OS and the functionality is part of the same endpoint agent. For all other files, Solution must classify the file based on file attributes (file location, file size, file name or based on logged in user etc.)

4.3.7 Solution should provide a breadth of tools that enable customers to detect sensitive data with Regex, Smart Regex, Categorization using Machine Learning (ML) and natural language processing capabilities do detect PCI, PII, etc., The solution should also be configured to detect specific keywords that may be critical for the Bank.

4.3.8 Solution must capture time sensitivity of a document. Example - Financial statement needs to be classified confidential until public release on 1st April and post that it should be classified as public.

4.3.9 The Bidder shall involve their resources in Data Collection, Policy/Rule Creation/Fine-Tuning, Policy/Rule Enforcement and Incident Management Support.

4.3.10 Bidder shall conduct awareness programs among end users as and when Bank requires.

Proposed Solution Shall duly meet the minimum technical requirements as specified in Annexure 1 – Minimum Technical requirement. The Bidder shall ensure that the bill of material is in compliance to the technical requirements

4.4 Database Activity Monitoring Solution (DAM)

Bank intends to address the database security concerns by implementing Database Activity Monitoring solution. This solution shall help in monitoring of all local, network and application level activities of the databases. Solution would run scheduled vulnerability scans for risk assessment and implement patches or apply virtual patches for all known vulnerabilities. The solution shall be implemented for different versions of databases & the servers on which the databases are running.

4.4.1 The Bidder is required to design & size the Database Activity Monitoring solution at DC and DRC for the proposed databases. The Bidder is also required to supply, install, configure and provide onsite comprehensive warranty & AMC/ATS services for the same over the tenure of the contract

4.4.2 The deployment & the coverage of the proposed solution shall be in line with the information provided by the Bank in the Clause 2.1 of this RFP

4.4.3 The Bidder is required to propose a database activity monitoring solution to ensure protection of all in scope databases security concerns of the Bank including:

a) Database Activity Monitoring
b) Vulnerability Assessment for Databases
c) Protection against un-patched Vulnerabilities

4.4.4 The Bidder is required to monitor all activities on the proposed database server

4.4.5 The Bidder is required to discover all critical databases and run scheduled vulnerability scans for risk assessment and implement patches or apply virtual patches for all known vulnerabilities.

4.4.6 The Bidder is required to implement database security tools which are able to identify end user information irrespective of how the data is being accessed.

4.4.7 The proposed solution shall have the following functionalities:

1. Ability to protect from all the proposed database threat vectors to meet RBI compliance requirements. Shall be able to capture all proposed database activities, including from across the network, from local users logged into the server itself, and even from inside the database itself via stored procedures or triggers.
2. Ability to monitor database activities from users using encrypted connections (example Oracle ASO, SSL, SSH etc.)
3. Deliver high performance without inducing any latency, and I/O overheads also shall not require any kernel changes or reboot.
4. Shall have support for virtualized environments
5. Shall be able to deploy quickly and non-intrusively, utilizing minimal resources.
6. Shall not have to use the native logging functionality of the database and use the shared memory for monitoring purposes.
7. Shall have ability to alert via inbuilt dashboard or any other tools. The solution shall also be able to prevent intrusion by terminating sessions and quarantine users that violate security policy.
8. Shall have ability to conduct a quick port scan providing database version and current patch status.
9. Shall have ability to present vulnerability assessment findings in preconfigured reports for various compliance standards.
10. Shall have ability to virtually Patch and protect sensitive proposed production databases without having to take them offline.
11. Shall have ability to protect proposed databases based on older DBMS versions that are no longer supported.
12. The solution’s database vulnerability manager shall automatically discover all databases versions of Oracle 8i, 9i, 10g, 11g ,12c and higher versions of Oracle , SQL Server 2000, 2005, 2008 and higher versions of SQL Server, Sybase, IBM DB2, my SQL including higher versions of the same and help bank to assess potential vulnerabilities
13. The solution’s database vulnerability management tool shall allow the user to perform a fully automated discovery of all existing databases within the Banks environment, along with a thorough scan to identify which of those contain

sensitive data such as payment card information, PAN numbers, phone numbers, and more.

14. The solution’s database vulnerability management tool shall also give bank detailed actionable information to help the bank prioritize and remediate those security gaps for compliance audits
15. The solution’s database vulnerability manager shall have maximum number checks for vulnerabilities as per the industry standards
16. The solution shall have checks like PCI DSS, STIG Benchmarks, Weak Passwords,Vulnerable Code, Data Discovery etc
17. The solution shall have a single browser based console for management and reporting.
18. The solution shall generate detailed reports, support custom generated reports, expert recommendations for remediation and also reduce time and effort preparing for and responding to compliance audits for the bank
19. Solution can be either software based or appliance based. In case of software based solution, the bidder shall size, supply and maintain the required hardware
20. Solution shall be able to receive feeds from a mirrored port as well as from the agents installed on the database servers.
21. For monitoring DBA activities, an agent shall be deployed on database servers and there shall be only one agent for monitoring DB activities including local DB traffic and the network DB traffic.
22. Agents shall have only minimal overhead for the production DB servers. The CPU utilization on the DB server shall not increase beyond 5% of the present utilization
23. Agent shall support different OS versions Windows, Unix, Linux and their different flavors.
24. Audit trail shall be stored within the solution in encrypted flat files and it shall not be stored in any database.
25. Solution shall have Database vulnerability assessment tests for assessing the vulnerabilities and mis-configurations of database servers, and their OS platforms. OSs and RDBMSs are required to be tested for known exploits and mis-configurations. The product shall identify missing patches.
26. The solution shall offer virtual patching capabilities (protecting the database from known vulnerabilities without deploying a patch or script on the system).
27. The product shall be configurable to function in sniffing (promiscuous) mode or inline mode.
28. Solution shall have built-in bypass for inline mode.
29. The solution shall not use the native database auditing functionality. The Solution shall not employ native database transaction log auditing.
30. Solution shall be able to integrate with the SIEM solution, Dashboard and Incident Management solution implemented at Bank.
31. The data transferred between the agent and the appliance shall be through an encrypted channel.
32. The solution shall capture at least the following activity by user/role
    a) Update, insert, delete(DML)
    b) Schema/Object changes(DDL)
    c) Manipulation of accounts, roles and privileges (DCL)
    d) Backend SQL query updates.

33. The solution shall be able to integrate with authentication systems like Active Directory / LDAP.
34. The solution shall function to support databases installed in virtual environment
35. Bidder must involve their resources in integration of databases, extracting & monitoring the alerts and regular follow-up with all the teams involved for closure of alerts
36. The Bidder shall provide the training of the deployed solution to the Bank personnel for 1 batch with 5 personnel.

The Database Activity Monitoring solution shall duly meet the minimum technical requirements as specified in Annexure 1 – Minimum Technical requirement. The Bidder shall ensure that the bill of material is in compliance to the technical requirements.

4.5 Endpoint Encryption (EE)

The Bank intends to procure Endpoint Encryption solution to be used for Laptops, tablets, mobile devices and critical desktops used by the Bank's end-users. The key purpose is to prevent unauthorized access from outsiders especially when a device is lost or stolen.

4.5.1 The Bidder is required to design & size the Endpoint Encryption solution. Currently Bank has about 1000 mobile devices including laptops, tablets, etc. which needs to be covered in this solution. The Bank envisages the increase in the number of such devices to 1500 during the tenure of 5 years. The bidders proposed solution shall be sized to meet the 5 year requirement. However, the solution shall be scalable to cover 3000 endpoints. Bidder is also required to supply, install, configure and provide onsite comprehensive warranty & AMC/ATS services for the same over the tenure of the contract.

4.5.2 Bidder has to migrate/decrypt the endpoints encrypted with existing solution and arrange for encryption with the bidder proposed solution.

4.5.3 The Bidder is required to implement Encryption on the devices identified by the Bank.

4.5.4 Bidder will be responsible for implementing & managing the policies defined by Bank for encryption.

4.5.5 The solution shall provide option for encryption of attached external storages or simply disconnect.

4.5.6 Bidder will give a brief introduction & mitigation steps to users using encryption. This will also cover but not be limited to various scenarios in case of lost password or theft of devices

4.5.7 Bidder will ensure a central helpdesk resource to cater to user issues on ongoing basis

4.5.8 Bidder will maintain the record of encrypted/non-encrypted endpoints and ensure compliance.

4.5.9 Bidder shall deploy their resources to handle Disk Encryption/Decryption Tasks and further technical/operational support.

4.5.10 The Bidder shall provide the administrative training of the deployed solution to the Bank personnel for 1 batch with 5 persons.

The proposed solution shall duly meet the minimum technical requirements as specified in Annexure 1 – Minimum Technical requirement

4.6 Patch Management Solution (PMS)

The Bank envisages the deployment of the Patch Management solution which shall provide an automated, simplified patching process and tool that is administered from a centralized browser based console. The centralized console shall be accessible from any location, from where Bank desire to access. The tool and process shall provide a unified, near real-time visibility and enforcement to deploy and manage patches to all distributed endpoints regardless of their location, connection type or status.

4.6.1 The Bidder is required to design & size the patch management solution to cover all the endpoints & servers located across all the Bank locations. Currently Bank has about 15000 endpoints including desktops, servers & laptops. The Bank envisages the increase in the number of end points to 25000 during the tenure of 5 years. The bidders proposed solution shall be sized to meet the 5 year requirement. However, the solution shall be scalable to cover 30000 endpoints. The Bidder's proposed solution shall be redundant and shall not have single point of failure.

4.6.2 The deployment & the coverage of the proposed solution shall be in line with the information provided by the Bank.

4.6.3 The Bidder is also required to supply, install, configure and provide onsite comprehensive warranty & AMC/ATS services for the same over the tenure of the contract.

4.6.4 The bidder shall provide onsite resources for administration of the solution which would include but not limited to day to day monitoring of the patch compliance, configuration, reporting, problem remediation, etc.

4.6.5 The Patch management solution shall provide the following functionality;

a) Automatically manage patches endpoints for multiple operating systems and applications, regardless of location, connection type or status.

b) Able to deploy customized packages (exe or MSI) through the solution in all endpoints as per bank requirement.

c) Enable automation to the level of correct patches to the correct endpoint.

d) Provide visibility into patch compliance with flexible, near real-time monitoring and reporting.

e) Provides near real-time visibility and control from a single management console.

f) Reduce security risk by streamlining and reducing remediation cycles

g) A Patch Management process & tool to be built with a focus of addressing Technical System and Software Vulnerabilities of the managed assets or endpoints (Desktops, Laptops, Servers)

h) The proposed patch management solution shall best fit within the present bandwidth deployed in Bank's corporate network.

i) Documenting Standards/ Procedures – Including Roles & Responsibilities, classification of critical & non-critical assets

j) Assessing Vulnerabilities of the managed endpoints or assets

k) Ascertaining a validity of the patch source

l) All Patches to have gone through a testing cycle

m) Methodology to ascertain whether a patch is required to be applied or not based on the business impact

n) Documenting timelines of applying patches based on criticality and adhering to the timelines

o) Comprehensive Patch Deployment options and documentation of the same

p) Identifying vulnerable assets and method to isolate until the vulnerability is addressed

q) Reporting of existing patches applied on the assets & software applications and report or provide alert for uninstalled patches.

r) Shall provide Real-time reporting information on which patches were deployed, when they were deployed, and who deployed them, as well as automatic confirmation that patches were applied for a complete closed-loop solution to the patching process

s) A single management server shall support up to 2,50,000 endpoints, shortening times for patches with no loss of endpoint functionality, even over low-bandwidth or globally distributed networks.

t) Research— the solution shall acquire, test, package and distribute many patch policies directly for end user. The solution shall reduce the patch management overhead of keeping track of what patches are released for which platform and when.

u) Assess—the solution shall continuously monitor and report endpoint state, including patch levels, to a management server. The solution shall also compare endpoint compliance against defined policies, such as mandatory patch levels as well as newly released patches.

v) Remediate— the solution shall be able to quickly create a report showing which endpoints need updates and then distribute those updates to the endpoints within minutes.

w) Confirm— once a patch is deployed, the solution shall automatically reassess the endpoint status to confirm successful installation and immediately updates the management server in real time. The operators shall be able to watch the patch deployment process in real time via a centralized management console to receive installation confirmation within minutes of initiating the patch process.

x) Enforce— the solution shall provide continuous endpoint enforcement and ensures that endpoints remain updated. If a patch is uninstalled for any reason, the solution shall automatically reapply it to the endpoint as needed.

y) Report—the solution shall provide web reporting capabilities to allow end users, administrators, executives, management and others to view dashboards and receive up- to-the-minute reports. Dashboards and reports shall indicate which patches were deployed, when they were deployed, who deployed them, and to which endpoints. The dashboards shall also show patch management progress in real time. The solution shall provide report of Last patch compliance status(Latest applied patches) of the managed assets or endpoints (Desktops, Laptops, Servers).

z) Alert: The solution shall provide alert whenever particular patch is removed or uninstalled from any machine integrated with patch management solution.

4.6.6 The Bidder shall provide the training of the deployed solution to the Bank personnel for 1 batch with 5 personnel in each batch.

4.6.7 The Patch Management solution shall duly meet the minimum technical requirements as specified in Annexure 1 – Minimum Technical requirement.

4.7 Facilities Management - Warranty/AMC/ATS Support service, People deployment & OEM Services of proposed solutions

4.7.1 Warranty/AMC/ATS Support service

4.7.1.1 The Bidder shall provide the maintenance (Warranty, AMC & ATS) for a period of Five years beginning from the date of acceptance of the solution by the Bank. The Warranty period for the new components shall be for the first Three years for Hardware & first year for Application software, for which the cost shall be factored in the respective hardware & application cost. The AMC/ATS shall be factored for the subsequent years for the tenure of the contract. The Bidder must factor the costs in the Bill of Material accordingly. As Bank is opting for subscription-based licenses, Bidder has to include the cost of AMC/ATS/Warranty in subscription cost. As part of warranty, AMC & ATS support the Bidder has to:

A. Provide on-site comprehensive support for Hardware equipment and software components provided as part of this RFP.

B. Tie back with respective OEMs for the maintenance services (Warranty/AMC/ATS).

C. Warrant all the Hardware equipment and software against defects arising out of faulty design, materials and media workmanship etc., for a period of FIVE years from the date of acceptance of the solutions by the Bank.

D. Provide for maintenance of Hardware equipment, including preventive maintenance support, as well as repair or replacement activity after a problem has occurred, If the supplied equipment are to be replaced permanently due to the Bidder’s inability to provide spares or maintain the equipment, the Bidder shall replace the equipment of same Make/ Model/configuration or of higher configuration. However, the Bank may accept different make/model/ configuration at its discretion if the original make/model/configurations are not available in the market due to obsolescence or technological upgradation.

E. Provide the support services like repair, replacement to resolve the problem as per the

Service levels defined in this RFP under Clause 7 ”Service Levels”

F. Defective Hardware equipment shall be replaced by the Bidder at their own cost, including the cost of transport etc. The Bidder shall not charge the Bank for any extra charges related to this activity.

G. Provide adequate spares for the critical components of the solution equipment.

H. Provide on-site support during quarterly DR drills or whenever required by the Bank. It is expected the vendor should participate in DR drill and ensure that the application switchover from DC to DR and vice versa happens during drill and disaster situation also.

I. Agree that the Bank will not be liable to pay any additional amounts in respect of any sort of maintenance covered under the scope of this tender during the tenure of the contract. Free on-site maintenance services shall be provided by the Bidder during the period of warranty.

J. Undertake system maintenance and replacement or repair of defective Hardware equipment.

K. In case equipment taken away for repairs, the Bidder shall provide similar standby equipment so that the equipment can be put to use in the absence of the originals/ replacements without disrupting the Bank’s regular work.

L. If during operation, the down time of any piece of equipment or component thereof does not prove to be within reasonable period, the Bidder shall replace the unit of component with another of the same performance and quality or higher, at no cost to the Bank.

M. Further provided that the Bank may, during the contract, shift the goods wholly or in part to other location(s) within the Country and in such case the Bidder undertakes to continue to warrant or maintain the goods at the new location without any other additional cost to the Bank.

N. In case the Bank desires to get the services delivered by their appointed service provider or System Integrator, then the OEM shall transfer such services to that preferred service provider or System Integrator at no additional cost to the Bank. A declaration to that effect from OEM shall be submitted by the bidder as per the format provided in Annexure 14 - Manufacturer Authorization.

O. In case of any issue with Hardware equipment and related software supplied by the Bidder, Bidder (who has supplied the Hardware equipment/software) shall log a call with OEM. It is the responsibility of the Bidder to resolve the issue with the assistance of the OEM where ever deemed necessary.

P. Provide all future software upgrades and patches for all components of the solution and assist the Bank or its System Integrator to install the same, if Bank desires during period of warranty, free of cost.

Q. The Bidder warrants that the Goods supplied under the Contract are new & unused, of the most recent or current models and incorporate all recent improvements in design and materials unless provided otherwise in the RFP.

R. The Bidder further warrants that all the Goods supplied under as part of this RFP shall have no defect arising from design, materials or workmanship (except when the design and/or material is required by the Bank's Specifications) or from any act or omission of the Bidder, that may develop under normal use of the supplied Goods in the conditions prevailing at the final destination.

4.7.2 People Deployment

4.7.2.1 The Bidder is required to deploy onsite people resource to provide L1, L2 & L3 level support to the proposed solutions for the tenure of the contract. Bank expects that bidders deploy their resources at the DC or any other location desired by the Bank and provide the remote support for any issues reported /logged by Bank's branches or locations other than DC. If the bidder's resources are unable to resolve the issues remotely then the bidder is expected to send the resource to the respective location to resolve the issue/event at no additional cost to the Bank.

4.7.2.2 The number of tentative resources indicated by the Bank in Annexure 15 – Resource Deployment Plan and Annexure 10 Commercial Bill of Material is for the purpose of the commercial normalization. The actual resources requirement would be finalized at the time of deployment & the same would be at the rate provided by the bidder in their commercial.

4.7.2.3 The Bidder shall provide the people deployment plan & profile of the people in Annexure 15

4.7.2.4 The expected skill & indicative scope for each level is as mentioned in Annexure 22: Resource Plan Matrix. Final selection of the resources would be done after interview with the Bank officials. The background verification of the selected resource would be the responsibility of the bidder. The bidder shall submit the background verification document as and when required by the Bank.

4.7.2.5 The attrition of resources shall be governed by the SLA mentioned in this RFP.

4.7.2.6 The Bank will perform the technical competency of the resources provided by the bidder either on its own or through third party resources. However, background verification and police verification of the resources shall be the responsibility of the bidder.

4.7.2.7 It is mandatory for the vendor to provide the dedicated onsite resources having the minimum detailed skill sets and experience as per **ANNEXURE 22**. The vendor personnel deployed in the Bank premises shall comply with the Bank's Information Security Requirements.

4.7.2.8 In case it is found either at the time of deployment or during the tenure of the project, that the appointed resource lacks the competency in particular aspect as mentioned above, the Bank may suggest the bidder for enhancement of skillset for that resource. The bidder will have to ensure that the resource obtain related certification/ knowledge within 3 months from being notified by the Bank. (Linked to SLA)

4.7.2.9 For Reporting and Timings the followings should be ensured.
i. The onsite team would report to Bank personnel / Bank authorized representative.

ii. The Team should operate from the Bank’s premises in Pune during the hours assigned to engineers as per the shifts
iii. In case of exigencies even during off business hours / Bank holidays, the resources may be required to be present onsite
iv. A replacement shall be given in case the resource proceeds for leave.

4.7.3 OEM Services

The Bidder is required to provide the assessment services from OEM for the proposed solutions.

The details of such services required to be delivered by the respective OEMs is detailed below.

4.7.3.1 OEM Scope of Work for Data Protection/Security Initiatives
It is Bidder’s responsibility to bring OEM’s Assessment Services as part of issued RFP by the Bank for this tender. The OEM or the 3rd party is required to provide the following services mentioned below as a part of the Architecture Assessment and provide the analysis report to the bank:

- One Time Security Assessment
- Yearly Security Assessment

4.7.3.1.1 One Time Security Assessment

- Conduct a gap analysis to identify gaps left after solution implementation
- Plug identified gaps in implemented solution
- Industry best practice implementation validation against implemented solution
- Design a strategy with support and visibility from senior management
- Enhance existing and develop new security policies, standards, guidelines and procedures for endpoint protection and built consensus and support for the new requirements within the organization
- Design a compliance communication and awareness program
- Enhance existing and develop new security policies, standards, guidelines and procedures for Data Classification
- Identify various compensating controls that address the protection of systems throughout its lifecycle
- Identify various controls that addressed the tactical implementation of proposed solutions.

4.7.3.1.2 Yearly Security Assessment

- Review and Update configuration rules & policies.
- Logging and Monitoring aspects, certification aspects, if involved,
- Conduct Maturity assessment
- Prepare the trainer material and arrange training for the bank for any updates in security policies.

5. Terms & Conditions

5.1 General

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

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

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

5.1.1 Rules for responding to this RFP

5.1.1.1 Refer to Table in "invitation of the Bidders" Clause of this RFP for last date for submission of the response to the RFP.

5.1.1.2 All responses shall be in English language. All responses by the Bidder to this RFP shall be binding on such Bidder for a period of 180 days after the opening of the commercial offer.

5.1.1.3 All responses including commercial and technical bids would be deemed to be irrevocable offers/proposals from the Bidder and may if accepted by the Bank form part of the final contract between the Bank and the selected Bidder. Bidder is requested to attach a letter from an authorized signatory attesting the veracity of information provided in the responses. Unsigned responses would be treated as incomplete and are liable to be rejected.

5.1.1.4 Any technical or commercial offer, submitted cannot be withdrawn / modified after the last date & time for submission of the bids unless specifically permitted by the Bank.

5.1.1.5 The Bidder may modify or withdraw its offer after submission, provided that, the Bank, prior to the closing date and time receives a written notice of the modification or withdrawal prescribed for submission of offers. No offer can be modified or withdrawn by the Bidder subsequent to the closing date and time for submission of the offers.

5.1.1.6 The Bidder is required to quote for all the components mentioned in the Scope of Work in this document. In case the Bidder does not quote for any of the components, the response would be deemed to include the quote for such unquoted components. It is mandatory to submit the compliance details in the formats in Annexure 10 Commercial Bill of Materials provided along with this document duly filled in, along with the Technical offer. The Bank reserves the right not to allow / permit changes in the technical specifications and not to evaluate the offer in case of non submission of the technical details in the required format or partial submission of technical details.

5.1.1.7 In the event the Bidder has not quoted for any mandatory items as required by the Bank and forming a part of the RFP circulated to the Bidder and responded to by the Bidder, the same will be deemed to be provided by the Bidder at no extra cost to the Bank.

5.1.1.8 The Bank ascertains and concludes that everything as mentioned in the RFPs circulated to the Bidder and responded by the Bidder has been quoted for by the Bidder, and there will be no extra cost associated with the same in case the Bidder has not quoted for any items or service that is required under this RFP.

5.1.1.9 All out of pocket expenses, travelling, boarding and lodging expenses for the entire life of the contract shall be a part of the financial offer submitted by the Bidder to the Bank. No extra costs on account of any items or services or by way of any out of pocket expenses, including travel, boarding and lodging etc. will be payable by the Bank. The Bidder cannot take the plea of omitting any charges or costs and later lodge a claim on the Bank for the same.

5.1.1.10 The Bidder at no point in time can excuse themselves from any claims by the Bank whatsoever for their deviations in confirming to the terms and conditions, payments schedules, time frame for supply of Security Software & Hardware and Patch Management solution etc. as mentioned in the RFP circulated by the Bank. Bidder shall be fully responsible for deviations to the terms & conditions, project schedule etc. as proposed in the RFP.

5.1.2 Price bid

5.1.2.1 The Bidder is requested to quote in Indian Rupees ('INR'). Bid in currencies other than INR would not be considered.

5.1.2.2 The prices quoted for the proposed solutions in the commercial bid shall be valid for the period of contract. In case there is decrease in the prices of the proposed solutions during the tenure of the contract; the cost benefit shall be passed to the bank

5.1.2.3 The prices quoted by the bidder shall include all applicable costs and taxes like GST, customs duty, excise duty, import taxes, freight, forwarding, insurance, delivery, installation, training etc. at the respective delivery location of the bank but exclusive of only applicable Service Tax and Octroi /Entry Tax / equivalent local authority cess, which shall be paid/ reimbursed on actual basis on production of bills.

5.1.2.4 In case of any variation (upward or down ward) in Government levies /GST/ taxes / cess / excise /custom duty etc. up-to the date of invoice, the benefit or burden of the same shall be passed on or adjusted to the Bank. The Bidder shall provide necessary documentary proof for the same.

Local entry taxes / octroi or Service Tax, whichever is applicable, if any, will be paid by the Bank on production of relative payment receipts / documents. If the Bidder makes any conditional or vague offers, without conforming to these guidelines, the Bank will treat the prices quoted as in conformity with these guidelines and proceed accordingly.

5.1.2.5 The price quoted by the bidder shall be inclusive of carrying out any mutually agreed changes to the deployed solutions- software or equipment that is required to be made in order to comply with any statutory or regulatory requirements or any industry-wide changes arising during the subsistence of this agreement, and the Bank shall not pay any additional cost for the same

5.1.3 Commercials

5.1.3.1. The Bank will consider the Total Cost of Ownership (TCO) over a five-year period.

5.1.3.2. Bidder is expected to maintain the proposed solutions supplied and commences the Warranty from the date of acceptance by the Bank. The Bidder shall be in a position to continue to provide AMC services as proposed to the Bank for the sixth and seven year on the sole discretion of the Approval granted by the Bank. The Bank in this regard shall take a decision based on the Bidder's performance.

5.1.3.3. Comprehensive annual maintenance charges must be quoted, on yearly basis, after taking due consideration for the warranty period.

5.1.3.4. The Bank has no obligation to accept the post warranty AMC services and the decision on the same would be taken towards the end of the warranty period.

5.1.3.5. They also have no obligation to buy the product & services mentioned as optional in commercial. However, such cost will be added in the TCO calculation.

5.1.3.6. While the Bank will summarily reject the equipment of a lower configuration than those mentioned in the Technical specifications, the Bank would accept equipment of higher configuration after price evaluation of such higher configuration to ensure that there is no adverse price impact and any advantage of a lower price in such cases is passed on to the Bank. The Bidder is not entitled to a longer period for delivery on the pretext of seeking approval from the Bank for a higher configuration or enhancement.

5.1.3.7. The insurance shall be for an amount equal to 110% of the total value of equipment on "all risks" basis, including war risks and theft and robbery and flood clauses, valid till the bank accepts the equipment. This will be applicable for the period of the contract.

5.1.3.8. The Price offer shall be on a **fixed price basis.** The rate quoted by the Bidder shall necessarily include the following:

1. Cost of the equipment;
2. Minimum of three years comprehensive Product warranty covering all parts, including adapters, chords etc., service, visits to the Bank DC, DRC, NS, SDCs, branches and other office Locations etc. In the event any of the Software & Hardware supplied by the Bidder reaches. End of Support during the contract period, the Bidder shall replace such Software & Hardware at no extra cost to the bank. The replaced Software & Hardware Infrastructure component shall be acceptable to the Bank.
3. Quarterly preventive maintenance of all the equipment to be supplied, which shall interlay, includes cleaning of inside and outside of all equipment during warranty period.
4. Transportation, forwarding and freight charges of all equipment to the site;
5. Comprehensive Insurance to cover equipment during transit period and until installation and acceptance of equipment by the Bank; the equipment shall be fully insured in Indian Rupees(INR) naming the Bank as the beneficiary and additional insured. In case any loss or damage occurs, the Bidder shall be responsible for initiating and pursuing claims and settlement and also make arrangements for repair and/or replacements of any damaged item/s;
6. All taxes, duties and levies of whatsoever nature excepting local entry taxes and Service Tax if any
7. Services, which are required to be extended by the Bidder in accordance with the terms and conditions of the contract.

5.1.3.9 The Bidder must provide and quote for all products and services as desired by the Bank as mentioned in this RFP.

5.1.3.10 In case there is a variation between numbers and words; the value mentioned in words would be considered.

5.1.3.11 The Bidder needs to provide Unit costs for components and services; unit rates would be considered for the TCO purposes

5.1.4 Performance Guarantee

5.1.4.1 If the contract is awarded, the Bidder shall furnish a Performance Guarantee to the extent of 15% of the value of the contract within 10 days of signing of the contract. The performance guarantee needs to be for the complete period of the contract and would need to be renewed till the expiry or termination of the contract. If the Performance guarantee is not submitted within 10 days, the Bank reserves the right to cancel the contract. The Performance Guarantee would be returned to the Bidder after the expiry or termination of the contract.

5.1.4.2 The project will be deemed complete only when all proposed solutions and related hardware & software contracted by the Bank are delivered in good condition, installed, implemented, tested and accepted along with the associated documentation.

5.1.4.3 Responses to this RFP shall not be construed as an obligation on the part of the Bank to award a contract for any services or combination of services. Failure of the Bank to select a Bidder shall not result in any claim whatsoever against the Bank and the Bank reserves the right to reject any or all bids in part or in full, without assigning any reason whatsoever. In the event of Bank not satisfied with the Price Discovery through this process, bank reserves the right to initiate the tendering process again through Limited or Open tender.

5.1.4.4 By submitting a proposal, the Bidder agrees to promptly contract with the Bank for any work awarded to the Bidder. Failure on the part of the awarded Bidder to execute a valid contract with the Bank will relieve the Bank of any obligation to the Bidder, and a different Bidder may be selected.

5.1.4.5 Any additional or different terms and conditions proposed by the Bidder would be rejected unless expressly assented to in writing by the Bank.

5.1.4.6 The Bidder must strictly adhere to the delivery dates or lead times identified in their proposal. Failure to meet these delivery dates, unless it is due to reasons entirely attributable to the Bank, may constitute a material breach of the Bidder’s performance. In the event that the Bank is forced to cancel an awarded contract (relative to this RFP) due to the Bidder’s inability to meet the established delivery dates, that Bidder will be responsible for any re-procurement costs suffered by the Bank. The liability in such an event could be limited to the amount actually spent by the Bank for procuring similar deliverables and services.

5.1.4.7 The Bidder represents and acknowledges to the Bank that it possesses necessary experience, expertise and ability to undertake and fulfil its obligations, under all the provisions of this RFP. The Bidder represents that all the deliverables to be supplied in response to this RFP shall meet the requirements of this scope.

5.1.4.8 The Bidder represents that the supplied equipment and documentation and/or use of the same by the Bank shall not violate or infringe the rights of any third party or the laws or regulations under any governmental or judicial authority. The Bidder further represents that the documentation to be provided to the Bank shall contain a complete and accurate description of the Equipment and other materials and services (as applicable), and shall be prepared and maintained in accordance with the highest industry standards. The Bidder represents and undertakes to obtain and maintain validity throughout the project, of all appropriate registrations permissions and approvals, which are statutorily required to be obtained by the Bidder for performance of the obligations of the Bidder. The Bidder further undertakes to inform and assist the Bank for procuring any registrations, permissions or approvals, which may at any time during the Contract Period be statutorily required to be obtained by the Bank for availing services from the Bidder.

5.1.4.9 All terms and conditions, payments schedules, time frame for all the deliverables as per this tender will remain unchanged unless explicitly communicated by the Bank in writing to the Bidder. The Bank shall not be responsible for any judgments made by the Bidder with respect to any aspect of the Assignment. The Bidder shall at no point be entitled to excuse themselves from any claims by the Bank whatsoever for their deviations in confirming to the terms and conditions, payments schedules, expected service levels, time frame for supply of proposed solutions, equipment etc. as mentioned in this RFP.

5.1.4.10 The Bank and the Bidder covenants and represents to the other Party the following:

It is duly incorporated, validly existing and in good standing under as per the laws of the state in which such Party is incorporated.

It has the corporate power and authority to enter into agreements and perform its obligations there under.

The execution, delivery and performance of terms and conditions under Agreements by such Party and the performance of its obligations there under are duly authorized and approved by all necessary action and no other action on the part of such Party is necessary to authorize the execution, delivery and performance under an Agreement. The execution, delivery and performance under an Agreement by such Party:

Will not violate or contravene any provision of its documents of incorporation;

Will not violate or contravene any law, statute, rule, regulation, licensing requirement, order, writ, injunction or decree of any court, governmental instrumentality or other regulatory, governmental or public body, agency or authority by which it is bound or by which any of its properties or assets are bound;

Except to the extent that the same have been duly and properly completed or obtained, will not require any filing with, or permit, consent or approval of or license from, or the giving of any notice to, any court, governmental instrumentality or other regulatory, governmental or public body, agency or authority, joint venture party, or any other entity or person whatsoever;

To the best of its knowledge, after reasonable investigation, no representation or warranty by such Party in this Agreement, and no document furnished or to be furnished to the other Party to this Agreement, or in connection herewith or with the transactions contemplated hereby, contains or will contain any untrue or misleading statement or omits or will omit any fact necessary to make the statements contained herein or therein, in light of the circumstances under which made, not misleading. There have been no events or transactions, or facts or information which has come to, or upon reasonable diligence, shall have come to the attention of such Party and which have not been disclosed herein or in a schedule hereto, having a direct impact on the transactions contemplated hereunder.

5.1.4.11 The Bidder undertakes to provide appropriate human as well as other resources required, to execute the various tasks assigned as part of the project, from time to time.

5.1.4.12 The Bank would not assume any expenses incurred by the Bidder in preparation of the response to this RFP and also would not return the offer documents to the Bidder.

5.1.4.13 The Bank shall not be held liable for costs incurred during any negotiations on proposals or proposed contracts or for any work performed in connection therewith.

5.1.5 Changes to the RFP

5.1.5.1 The Bank also reserves the right to change any terms and conditions of the RFP and its subsequent addendums as it deems necessary at its sole discretion. The bank will inform the Bidder about changes, if any before the commercial bids are opened.

5.1.5.2 The Bank may revise any part of the RFP, by providing an addendum to the Bidder at stage till commercial bids are opened. The Bank reserves the right to issue revisions to this RFP at any time before the opening of the commercial bid.

5.1.5.3 The Bank reserves the right to extend the dates for submission of responses to this document.

5.1.5.4 Bidder shall have the opportunity to clarify doubts pertaining to the RFP in order to clarify any issues they may have, prior to finalizing their responses. All queries/questions are to be submitted to the Bank coordinator and shall be received at the address & time mentioned in clause 1. Responses to inquiries and any other corrections and amendments will be distributed to the Bidder by fax or in electronic mail format or hardcopy letter or will be uploaded on website, at the sole discretion of the Bank.

5.1.5.5 Preliminary Scrutiny – The Bank will scrutinize the offer to determine whether it is complete, whether any errors have been made in the offer, whether required technical documentation has been furnished, whether the documents have been properly signed, and whether items are quoted as per the schedule. The Bank may, at its discretion, waive any minor non-conformity or any minor deficiency in an offer. This shall be binding on the Bidder and the Bank reserves the right for such waivers and the Banks decision in the matter will be final.

5.1.5.6 Clarification of Offer – To assist in the scrutiny, evaluation and comparison of offer, the Bank may, at its discretion, ask the Bidder for clarification of their offer. The Bank has the right to disqualify the Bidder whose clarification is found not suitable to the proposed project.

5.1.5.7 The Bank reserves the right to make any changes in the terms and conditions of purchase. The Bank will not be obliged to meet and have discussions with any Bidder, and / or to listen to any representations.

5.1.5.8 Erasures or Alterations – The offer containing erasures or alterations will not be considered. There shall be no hand-written material, corrections or alterations in the offer. Technical details must be completely filled up. Correct technical information of the product being offered must be filled in. Filling up of the information using terms such as “OK”, “accepted”, “noted”, “as given in brochure / manual” is not acceptable. The Bank may treat the offers not adhering to these guidelines as unacceptable.

5.1.5.9 Pricing – It is absolutely essential for the Bidder to quote the lowest price at the time of making the offer in its own interest. In the event of Bank not satisfied with the Price Discovery in this process, bank reserves the right to initiate the tendering process again through Limited or Open tender for any solution which is part of the scope of work

5.1.5.10 Right to Alter Quantities – The Bank reserves the right to alter the requirements specified in the tender. The Bank also reserves the right to delete or increase one or more items from the list of items specified in the tender. The bank will inform the Bidder about changes, if any. In the event of any alteration in the quantities the price quoted by the Bidder against the item would be considered for such alteration. The Bidder agrees that the prices quoted for each line item & component is valid for period of contract and can be used by Bank for alteration in quantities. Bidder agrees that there is no limit on the quantities that can be altered under this contract. During the contract period the Bidder agrees to pass on the benefit of reduction in pricing for any additional items to be procured by the Bank in the event the market prices / rate offered by the Bidder are lower than what has been quoted by the Bidder as the part of commercial offer. Any price benefit in the proposed solution equipment, licenses, services & equipment shall be passed on to the Bank within the contract period.

5.1.5.11 Details of Sub-contracts, as applicable – If required by the Bank, Bidder shall provide complete details of any subcontractor/s used for the purpose of this engagement. It is clarified that notwithstanding the use of sub-contractors by the Bidder, the Bidder shall be solely responsible for performance of all obligations under the RFP irrespective of the failure or inability of the subcontractor chosen by the Bidder to perform its obligations. The Bidder shall also have the responsibility for payment of all dues and contributions, as applicable, towards statutory benefits for its employees and sub-contractors.

5.1.5.12 No Proposed solution will be accepted as complete if any components of Hardware or software are not delivered. In such an event, the supply will be termed incomplete and will not be accepted and warranty period will not commence besides Bank's right to invoke the penalties which will be prescribed in the contract.

5.1.5.13 There will be an inspection test conducted by the Bank after installation of the proposed solutions. In case of discrepancy in Proposed solution equipment supplied & not matching the Bill of Materials or technical proposal submitted by the Bidder in their technical bid, the Bidder shall be given 6 weeks' time to correct the discrepancy post which Bank reserves the right to cancel the entire contract and the Bidder shall take back their equipment at their costs and risks. The inspection test will be arranged by the Bidder at the sites in the presence of the officials of the Bank. The warranty for the equipments (including software and hardware provided by the Bidder pursuant to this Agreement) will commence after acceptance sign off. The tests will involve trouble-free operation of the complete system during inspection apart from physical verification and testing. There shall not be any additional charges for carrying out this inspection test. The Bank will take over the system on successful completion of the above acceptance test. The Installation cum Inspection Test & Check certificates jointly signed by Bidder's representative and Bank's official shall be received at along with invoice etc. for scrutiny before taking up the request for consideration of payment.
5.1.5.14 The Head Office of the Bank is floating this RFP. However, the Bidder(s) getting the contracts shall install and commission the equipment, procured through this RFP, at the Bank's Datacenters – DC, DR & NS and branches or at such centres as the Bank may deem fit and the changes, if any, in the locations will be intimated to the Bidder.
5.1.5.15 The Bank shall inform the Bidder all breaches and claims of indemnification and shall grant the Bidder sole authority to defend, manage, negotiate or settle such claims; and make available all reasonable assistance in defending the claims (at the expense of the Bidder). The written demand by the Bank as to the loss / damages mentioned above shall be final, conclusive and binding on the Bidder and Bidder shall be liable to pay on demand the actual amount of such loss / damages caused to the Bank.

In respect of demands levied by the Bank on the Bidder towards breaches, claims, etc. the Bank shall provide the Bidder with details of such demand levied by the Bank. However, there are other indemnities such as indemnity for IPR violation, confidentiality breach, etc., that the Bidder is expected to provide as per the RFP.

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

5.1.5.16 The Bidder's representative and local office at Pune will be the contact point for the bank. The delivery status of equipment shall be reported on a weekly basis.

5.1.5.17 Bidder shall ensure that the Proposed solution equipment/ and its associated components delivered to the Bank including all components and attachments are brand new. In case of software supplied with the system, the Bidder shall ensure that the same is licensed and legally obtained with valid documentation made available to the Bank.

5.1.5.19 Manufacturer's Authorization Form – The Bidder shall furnish a letter from original equipment manufacturer in the format provided in Annexure 14 - Manufacturer Authorization provided along with this RFP,

5.1.5.20 Technical Inspection and Performance Evaluation - The Bank may choose to carry out a technical inspection/audit and performance evaluation of products offered by the Bidder. The Bidder would permit the Bank or any person / persons appointed by the Bank to observe the technical and performance evaluation / benchmarks carried out by the Bidder. Any expenses (performing the benchmark, travel, stay, etc.) incurred for the same would be borne by the Bidder and under no circumstances the same would be reimbursed to the Bidder by the Bank.

5.1.6 Conditional bids

Conditional bids shall not be accepted on any ground and shall be rejected straightway. If any clarification is required, the same shall be obtained before submission of bids.

5.1.7 Award of Contract

5.1.7.1 The Bank will award the contract to the successful Bidder, out of the Bidders who have responded to Bank's tender as referred above, who has been determined to qualify to perform the contract satisfactorily, and whose Bid has been determined to be substantially responsive, and is the lowest commercial Bid.

5.1.7.2 The Bank reserves the right at the time of award of contract to increase or decrease of the quantity of goods or services or change in location where equipment are to be supplied from what was originally specified while floating the tender without any change in unit price or any other terms and conditions.

5.1.8 Bid Security

a) The Bidder shall furnish, as part of its Technical bid, bid security of an amount of Rs. 50,00,000/-(Rupees Fifty Lakhs Only). The bid security is required to protect the Bank against the risk of Bidder's Conduct. The bid security shall be denominated in the INDIAN RUPEES only and shall be in the form of a Demand Draft favoring "Bank of Maharashtra" by a Scheduled Commercial Bank or a Foreign bank located in India in the form provided in Annexure 9 of this RFP Any bid not secured in accordance with the above will be rejected by the Bank as non-responsive.

b) Unsuccessful Bidders' bid security will be discharged/returned as promptly as possible after the expiration of the period of bid validity prescribed by the Bank.

c)The successful Bidder’s bid security will be discharged upon the Bidder signing the Contract and furnishing the performance guarantee.

The bid security may be forfeited:

(a) If Bidder withdraws its bid during the period of bid validity specified by the Bidder on the Bid Form;

Or

(b) In case of the successful Bidder, if the Bidder fails:
(i) To sign the Contract
And
(ii) To furnish performance security.

c) Period of Validity of Bids

The process of bid evaluation, approval and the subsequent activities may be assumed to take a reasonable amount of time. Therefore, the bids shall remain valid for 180 days after the date of opening of Commercial Bid prescribed by the Bank. A bid valid for a shorter period shall be rejected by the Bank as non-responsive.

5.1.9 Confidentiality Agreement

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

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

5.2 Terms of Reference (‘ToR’)

5.2.1 Contract Commitment

The Bank intends that the contract, which is contemplated herein with the Bidder, shall be for a period of five years from the date of acceptance sign off. However, the extension of the AMC post warranty period will be at the sole discretion of the Bank.

The Bidder will continue to provide AMC services to the Bank for the fourth and fifth year on the sole discretion of the Approval granted by the Bank. The Bank in this regard shall continue with the Bidder services based on their satisfaction of the Bidder’s performance.

5.2.2 Ownership, Grant and Delivery

The Bidder shall procure and provide a non-exclusive, non-transferable, perpetual license for all the software to be provided as a part of this project. All the licenses shall be purchased in the name of the Bank. The use of software by Bidders on behalf of the Bank would be considered as use thereof by the Bank and the software shall be assignable / transferable to any successor entity of the Bank.

The bank reserves the right to use the excess capacity of the proposed solution equipment, licenses and other infrastructure supplied by the Bidder for any internal use of the Bank or its affiliates, subsidiaries or regional rural bank at no additional cost. The Bidder agrees that they do not have any reservations on such use and will not have any claim whatsoever against such use of the proposed solutions equipment, licenses and infrastructure by the Bank.

Further the Bidder also agrees that such use will not infringe or violate any license or other requirements.

5.2.3 Completeness of the Project

The project will be deemed as incomplete if the desired objectives of the project **Clause - 4 Scope of Work** of this document are not achieved.

5.2.4 Inspection

The Bank will carry out the inspection tests for testing of related deliverables & licenses to verify that the supplied equipments are as per the Bill of materials. The Bidder shall assist the Bank in all inspection tests to be carried out by the Bank.

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

The Installation cum Inspection Test and Check certificates jointly signed by representative of the Bidder and official auditor appointed by the Bank will be received at Head Office of the Bank along with Bidder invoice for scrutiny before taking up the request for consideration of payment.

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

5.2.5 Inspection Certificate

On successful completion of inspection testing i.e. receipt of deliverables, installation & configuration of the proposed solution etc. and the Bank is satisfied with the working on the system, the inspection certificate will be jointly prepared with the selected Bidder at the time of the execution of the project.

The date on which such certificate is signed by the Bank shall be deemed to be the date of acceptance of the system and the Warranty of the system starts from that date.

5.2.6 Compliance and assurance

i. Assisting the Bank in attaining and ensuring ongoing compliance to various regulatory and data security/ privacy requirements.

ii. Addressing relevant threats/ risks identified in a proactive manner and through audit observations.
iii. Providing analysis and MIS for solution and associated services related data, to demonstrate audit readiness and adherence to the agreed service levels.
iv. For all existing applications, SI shall submit Data Dictionary (wherever feasible) as a part of System documentations.
v. SI shall submit within 10 days from signing of this agreement, an Application Integrity Statement from application system vendor providing reasonable level of assurance about the application being free of malware at the time of sale, free of any obvious bugs and free of any covert channels in the code.

5.2.7 Assignment

Bank may assign the proposed solution equipment and related software provided therein by the Bidder in whole or as part of a corporate reorganization, consolidation, merger, or sale of substantially all of its assets. The Bank shall have the right to assign such portion of the AMC services to any of the sub-contractors, at its sole option, upon the occurrence of the following:

(i) Bidder refuses to perform;
(ii) Bidder is unable to perform;
(iii) Termination of the contract with the Bidder for any reason whatsoever;
(iv) Expiry of the contract. Such right shall be without prejudice to the rights and remedies, which the Bank may have against the Bidder.

The Bidder shall ensure that the said subcontractors shall agree to provide such services to the Bank at no less favourable terms than that provided by the Bidder and shall include appropriate wordings to this effect in the agreement entered into by the Bidder with such sub-contractors. The assignment envisaged in this scenario is only in certain extreme events such as refusal or inability of the Bidder to perform or termination/expiry of the contract.

5.2.8 Insurance

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

The Bidder shall furnish to the Bank prior to the commencement of the supply of solution equipment, copies of the certificates of insurance as stipulated as set out herein certifying that the policies of insurance, endorsed as required, are in full force and effect (together with any required waivers of subrogation). The Bidder shall ensure that the policies contain provision that the Bank will be given thirty (30) days' prior written notice by the insurers in the event of either cancellation or material change in coverage; and that the Bank shall be given thirty (30) days' notice prior to termination of the insurance for failure to renew or pay premium. The Insurance procured by the Bidder shall be primary to any other insurance available to the Bank, its assigns, officers, directors, agents and employees.
The Bidder's obligation to maintain insurance coverage hereunder shall be in addition to, and not in lieu of, the Bidder's other obligations, and the Bidder's liability to the Bank shall not be limited to the amount of coverage.

It is usual for Bidders to have name of their customers endorsed as additional insured / beneficiary and provide a copy of the policy to the customers.
The Bank shall be added as a “Beneficiary or additional insured” and appropriate certification shall be provided by the Bidder’s insurer certifying compliance with the provisions of this clause

5.2.9 Order Cancellation

The Bank reserves its right to cancel the order in the event of one or more of the following situations, that are not occasioned due to reasons solely and directly attributable to the Bank alone:

5.2.9.1 Inordinate delays & lack of action from the Bidder towards supply and delivery beyond the delivery timelines.

5.2.9.2 Inability of the Bidder to remedy the situation within 60 days from the date of pointing out the defects by the Bank. (60 days will be construed as the notice period)

5.2.9.3 In case of order cancellation, the Bidder agrees that they will bear the complete cost of any reprocurement that would be needed by the Bank to fulfil the obligations of the RFP.

5.2.10 Indemnity

5.2.10.1 SI shall indemnify, protect and save the Bank and hold the Bank harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings, (including reasonable attorney fees), relating to or resulting directly or indirectly from:
i. an act or omission of the SI, its employees, its agents, or employees of the consortium in the performance of the services provided by this Agreement,
ii. breach of any of the terms of this Agreement and amendments thereof or breach of any representation or warranty by the SI,
iii. use of the provided Solution and/ or facility provided by the SI,
iv. infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components used to facilitate and to fulfill the scope of the Solution requirement.

5.2.10.2 The SI shall further indemnify the Bank against any loss or damage arising out of loss of data, claims of infringement of third-party copyright, patents, or other intellectual property, and third party claims on the Bank for malfunctioning of the equipment/s providing facility to Bank’s equipment at all points of time, provided however,
i. the Bank notifies the SI in writing immediately on aware of such claim,
ii. the SI has sole control of defense and all related settlement negotiations,
iii. the Bank provides the SI with the assistance, information and authority reasonably necessary to perform the above, and
iv. the Bank does not make any statement or comments or representations about the claim without prior written consent of the SI, except under due process of law or order of the court.
It is clarified that the SI shall in no event enter into a settlement, compromise or make any statement (including failure to take appropriate steps) that may be detrimental to the Bank’s (and/or its customers, users and SIs) rights, interest and reputation.

5.2.10.3 The SI shall indemnify the Bank (including its employees, directors or representatives) from and against claims, losses, and liabilities arising from:
i. Non-compliance of the SI with Laws / Governmental Requirements
ii. IP infringement

iii. Negligence and misconduct of the SI, its employees, and agents
iv. Breach of any terms of this Agreement or the Agreement and amendments thereof or Representation made by the SI
v. Act or omission in performance of service.
vi. Loss of data due to SI provided facility provided the loss can directly and solely be attributable due to services provided by SI
vii. Death or personal injury caused by the negligence of the indemnifying party, its personnel or its subcontractor.
viii. Except to the extent attributable to a breach of contract by, willful, negligent or unlawful act or omission of the successful bidder or a third party which is controlled by the Bidder as governed by Indian IT Act.
ix. The breach by the Bidder of any of its obligations under Confidentiality."

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

5.2.10.5 The SI shall not indemnify the Bank for:
i. Any loss of profits, revenue, contracts, or anticipated savings or
ii. Any consequential or indirect loss or damage however caused, provided that the claims against customers, users and SIs of the Bank would be considered as a "direct" claim.

5.2.11 Inspection of Records

All Bidder records with respect to any matters covered by this tender shall be made available to the Bank or its designees at any time during normal business hours, as often as the Bank deems necessary, to audit, examine, and make excerpts or transcripts of all relevant data. Said records are subject to examination. The cost of the audit will be borne by the Bank. The scope of such audit would be limited to Service Levels being covered under the contract, and financial information would be excluded from such inspection, which will be subject to the requirements of statutory and regulatory authorities.

5.2.12 Publicity

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

5.2.13 Solicitation of Employees

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

5.2.14 Penalty

5.2.14.1 The Bank expects the Bidder to complete the scope of the project as mentioned in clause 4 -scope of work of this document within the timeframe specified in Clause 2.3.1 Project Timelines of this document. Inability of the Bidder to either provide the requirements as per the scope or to meet the timelines as specified would be treated as breach of contract and would invoke the penalty clause.

5.2.14.2 For example, if the Bidder is not able to supply a Proposed solution equipment or the supplied equipment requires some more parts for its functioning or there is a delay in installation of any equipment then the penalty levied will be 1% of the cost of “That Proposed solution component” per week of delay. For example there is delay of two week in delivery / installation of an equipment ; then the penalty will be charged 2% of the cost of that equipment.

5.2.14.3 The proposed rate of penalty would be 1 % of the of value of affected service or product per week of non-compliance to, the service levels for every percentage below the expected levels of service, for that particular service. Overall cap for penalties will be 10% of the contract value. Thereafter, the contract may be cancelled and amount paid if any, will be recovered with 1.25% interest per month. The bank also has the right to invoke the performance guarantee. Refer to Annexure 10 – Commercial Bill of Materials for cost of the product and services; also refer to clause 2.3.1 for project timelines.

5.2.14.4 Inability of the Bidder to provide services at the service levels defined would result in breach of contract and would invoke the penalty clause. Refer to clause 7 for service levels and service credits

5.2.14.5 Notwithstanding anything contained above, no such penalty will be chargeable on the Bidder for the inability occasioned, if such inability is due to reasons entirely attributable to the Bank.

5.2.14.6 Notwithstanding what is mentioned hereinabove or anywhere else in the tender, the maximum amount that may be levied by way of penalty shall on no account exceed 10 % of the Total Contract value and the contract value will be determined at the time of contract finalization.

5.2.15 Information Ownership

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

5.2.16 Sensitive Information

Any information considered sensitive must be protected by the Bidder from unauthorized disclosure, modification or access.

Types of sensitive information that will be found on Bank’s system the Bidder may support or have access to include, but are not limited to: Information subject to special statutory protection, legal actions, disciplinary actions, complaints, IT security, pending cases, civil and criminal investigations, etc.

5.2.17 Privacy & Security Safeguards

The Bidder shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the

Bidder under this contract or existing at any Bank location. The Bidder shall develop procedures plans to sure that IT resources leaving the control of the assigned user (such as being reassigned, removed for repair, replaced, or upgraded) are cleared of all Bank data and sensitive application software. The Bidder shall also ensure that all subcontractors who are involved in providing such security safeguards or part of it shall not publish or disclose in any manner, without the Bank's prior written consent, the details of any security safeguards designed, developed, or implemented by the Bidder under this contract or existing at any Bank location.

5.2.18 Confidentiality

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

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

Responses received become the property of Bank and cannot be returned. Responses will not be used and shared with third party for any means. Information provided by each bidder will be held in confidence, and will be used for the sole purpose of evaluating a potential business relationship with the bidder.

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

(a) Relates to the Disclosing Party; and

(b) is designated by the Disclosing Party as being confidential or is disclosed in circumstances where the Receiving Party would reasonably understand that the disclosed information would be confidential or

(c) Is prepared or performed by or on behalf of the Disclosing Party by its employees, officers, directors, agents, representatives or consultants

(d) Without limiting the generality of the foregoing, Confidential Information shall mean and include any information, data, analysis, compilations, notes, extracts, materials, reports, drawings, designs, specifications, graphs, layouts, plans, charts, studies, memoranda or other documents, or materials that may be shared by Bank with the bidder to host Bank’s equipment at the site

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

(f) Information disclosed pursuant to this clause will be subject to confidentiality forever.

1. The Receiving Party shall, at all times regard, preserve, maintain and keep as secret and confidential all confidential information and confidential materials of the Disclosing Party howsoever obtained and agrees that it shall not, without obtaining the written consent of the Disclosing Party:
2. Unless otherwise agreed herein, use any such confidential information and materials for its own benefit or the benefit of others or do anything prejudicial to the interests of the Disclosing Party or its customers or their projects.
3. In maintaining confidentiality hereunder the Receiving Party on receiving the confidential information and materials agrees and warrants that it shall:
    - Take at least the same degree of care in safeguarding such confidential information and materials as it takes for its own confidential information of like importance and such degree of care shall be at least, that which is reasonably calculated to prevent such inadvertent disclosure;
    - Keep the confidential information and confidential materials and any copies thereof secure and in such a way so as to prevent unauthorized access by any third party;
    - Limit access to such confidential information and materials to those of its directors, partners, advisers, agents or employees, sub-contractors and contractors who are directly involved in the consideration/evaluation of the confidential information and bind each of its directors, partners, advisers, agents or employees, sub-contractors and contractors so involved to protect the confidential information and materials in the manner prescribed in this document; and
    - Upon discovery of any unauthorized disclosure or suspected unauthorized disclosure of confidential information, promptly inform the Disclosing Party of such disclosure in writing and immediately return to the Disclosing Party all such Information and materials, in whatsoever form, including any and all copies thereof.
4. The Receiving Party who receives the confidential information and materials agrees that on receipt of a written demand from the Disclosing Party:
    a. Immediately return all written confidential information, confidential materials and all copies thereof provided to, or produced by it or its advisers, as the case may be, which is in Receiving Party’s possession or under its custody and control;

    b. To the extent practicable, immediately destroy all analyses, compilations, notes, studies, memoranda or other documents prepared by it or its advisers to the extent that the same contain, reflect or derive from confidential information relating to the Disclosing Party;

    c. So far as it is practicable to do so immediately expunge any confidential information relating to the Disclosing Party or its projects from any computer, word processor or other device in its possession or under its custody and control; and

    d. To the extent practicable, immediately furnish a certificate signed by its director or other responsible representative confirming that to the best of his/her knowledge, information and belief, having made all proper enquiries the requirements of this paragraph have been fully complied with.
5. The restrictions in the preceding clause shall not apply to:
    a. Any information that is publicly available at the time of its disclosure or becomes publicly available following disclosure (other than as a result of disclosure by the Disclosing Party contrary to the terms of this document); or any information which

is independently developed by the Receiving Party or acquired from a third party to the extent it is acquired with the valid right to disclose the same.

b. Any disclosure required by law or by any court of competent jurisdiction, the rules and regulations of any recognized stock exchange or any enquiry or investigation by any governmental, statutory or regulatory body which is lawfully entitled to require any such disclosure provided that, so far as it is lawful and practical to do so prior to such disclosure, the Receiving Party shall promptly notify the Disclosing Party of such requirement with a view to providing the Disclosing Party an opportunity to obtain a protective order or to contest the disclosure or otherwise agree to the timing and content of such disclosure.

c. The confidential information and materials and all copies thereof, in whatsoever form shall at all times remain the property of the Disclosing Party and its disclosure hereunder shall not confer on the Receiving Party any rights whatsoever beyond those contained in this document.

d. The confidentiality obligations shall survive the expiry or termination of the agreement between the bidder and the Bank.

Source Code

a) The application software should mitigate Application Security Risks, at a minimum, those discussed in OWASP top 10 (Open Web Application Security Project).The Bank shall have right to audit of the complete solution proposed by the bidder, and also inspection by the regulators of the country. The Bank shall also have the right to conduct source code audit by third party auditor.

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

c) In case the Bidder is coming with software which is not its proprietary software, then the Bidder must submit evidence in the form of agreement it has entered into with the software vendor which includes support from the software vendor for the proposed software for the full period required by the Bank.

5.2.19 Technological Advancements

The Bidder has to ensure that the equipment supplied are not declared as end of sale for at least 12 months from the date of the submission of the offer. The Bidder also has to ensure that the equipment supplied as part of this bid are not declared end of support or services for at least 7 years from the date of submission of bid. The Bidder agrees that all parts & spares for the equipment would be made available during the period of the contract. It will be the obligation of the Bidder to provide a minimum of 1 year notice before any equipment is to be declared as end of support or sale

5.2.20 ISMS Framework

The bidder shall abide by the ISMS framework of the Bank. Bidder shall abide by the ISMS policy and any other policy and subsequent procedures of the Bank.

5.2.21 IPv6 readiness

The SI shall ensure that the all the solutions including hardware and software are IPv6 compatible and shall ensure the readiness as per the national roadmap for IPv6 deployment at no extra cost to the Bank. SI shall successfully pass both Interoperability and Conformance tests for IPV6 and shall receive the IPV6 Ready Logo. The SI shall ensure that the devices used for the entire solution and related services shall be on the IPv6 Ready logo program approved list and shall pass the IPv6 Ready Logo Phase-2 test.

5.2.22 IT ACT

The bidder must ensure that the proposed products/services are compliant to all such applicable existing regulatory guidelines of GOI / RBI and also adheres to requirements of the IT Act 2000 (including amendments in IT Act 2008) and Payment and Settlement Systems Act 2007 and amendments thereof as applicable. The bidder must submit a self-declaration to this effect.

The successful bidder shall indemnify, protect and save Bank against all claims, losses, costs, damages, expenses, action, suits and other proceedings, resulting from infringement of any patent, trademarks, copyrights etc. or such other statutory infringements under the Copyrights Act, 1957 or IT Act 2008 or any Act in force at that time in respect of all the hardware, software and network equipment or other systems supplied by the bidder to Bank from any source.

5.2.23 Aadhar Act

The successful bidder must comply with Aadhar Act 2016 and the subsequent amendments as applicable to the products/services.

5.2.24 Bidder’s Liability

The Bidder’s aggregate liability in connection with obligations undertaken as a part of the RFP regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), shall be at actual and limited to the value of the contract. The Bidder’s liability in case of claims against the Bank resulting from misconduct or gross negligence of the Bidder, its employees and subcontractors or from infringement of patents, trademarks, copyrights or such other Intellectual Property Rights or breach of confidentiality obligations shall be unlimited. The Bank shall not be held liable for and is absolved of any responsibility or claim/litigation arising out of the use of any third party software or modules supplied by the Bidder as part of this RFP. In no event shall either party be liable for any indirect, incidental or consequential damages or liability, under or in connection with or arising out of this agreement or the Proposed solution components, hardware or the software delivered hereunder, howsoever such liability may arise, provided that the claims against customers, users and Bidders of the Bank would be considered as a direct claim.

5.2.25 Guarantees

Bidder shall guarantee that the software and allied components used to service the Bank are licensed and legal. All Proposed solution and related component must be supplied with their original and complete printed documentation.

5.2.26 Force Majeure

1. The bidder shall not be liable for forfeiture of its performance security, liquidated damages or termination for default, if any to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure.

2. For purposes of this clause, "Force Majeure" means an event explicitly beyond the reasonable control of the bidder and not involving the bidder's fault or negligence and not foreseeable. Such events may include act of God, governmental act, political instability, epidemic, pandemic, flood, fire, explosion, accident, civil commotion, war, computer viruses, industrial dispute, labour unrest and any other occurrence of the kind listed above, which is not reasonably within the control of the affected party.
3. Each Party agrees to give to the other a notice of fifteen calendar days from the date of such occurrence of the incident or notification etc. by Govt. as applicable and such notice shall contain details of the circumstances giving rise to the event of Force Majeure. Unless otherwise directed by Bank in writing, the bidder shall continue to perform bidder's obligations under the contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.
4. In such a case the time for performance shall be extended by a period (s) not less than duration of such delay. If the duration of delay continues beyond a period of three months, Bank and the bidder shall hold consultations in an endeavor to find a solution to the problem.

5.2.27 Resolution of Disputes

5.2.27.1 The Bank and the supplier Bidder shall make every effort to resolve amicably, by direct informal negotiation between the respective project directors of the Bank and the Bidder, any disagreement or dispute arising between them under or in connection with the contract.

5.2.27.2 If the Bank project director and Bidder project director are unable to resolve the dispute after thirty days from the commencement of such informal negotiations, they shall immediately escalate the dispute to the senior authorized personnel designated by the Bidder and Bank respectively.

5.2.27.3 If after thirty days from the commencement of such negotiations between the senior authorized personnel designated by the Bidder and Bank, the Bank and the Bidder have been unable to resolve amicably a contract dispute; either party may require that the dispute be referred for resolution through formal arbitration. The language of the Arbitration proceeding be in English.

5.2.27.4 All questions, disputes or differences arising under and out of, or in connection with the contract or carrying out of the work whether during the progress of the work or after the completion and whether before or after the determination, abandonment or breach of the contract shall be referred to arbitration by a sole Arbitrator: acceptable to both parties OR the number of arbitrators shall be three, with each side to the dispute being entitled to appoint one arbitrator. The two arbitrators appointed by the parties shall appoint a third arbitrator shall act as the chairman of the proceedings. The award of the Arbitrator shall be final and binding on the parties. The Arbitration and Reconciliation Act 1996 or any statutory modification thereof shall apply to the arbitration proceedings and the venue of the arbitration shall be Pune.

5.2.27.5 If a notice has to be sent to either of the parties following the signing of the contract, it has to be in writing and shall be first transmitted by facsimile transmission by postage prepaid registered post with acknowledgement due or by a reputed courier service, in the manner as elected by the Party giving such notice. All notices shall be deemed to have been validly given on

(i) the business date immediately after the date of transmission with confirmed answer back, if transmitted by facsimile transmission, or

(ii) the expiry of five days after posting if sent by registered post with A.D., or

(iii) the business date of receipt, if sent by courier.

5.2.27.6 This RFP shall be governed and construed in accordance with the laws of India. The courts of Pune alone and no other courts shall be entitled to entertain and try any dispute or matter relating to or arising out of this RFP. Notwithstanding the above, the Bank shall have the right to initiate appropriate proceedings before any court of appropriate jurisdiction, shall it find it expedient to do so.

5.2.28 Exit Option and Contract Re-Negotiation

5.2.28.1 The Bank reserves the right to cancel the contract in the event of happening one or more of the following Conditions:
5.2.28.1.1 Failure of the successful Bidder to accept the contract and furnish the Performance guarantee within 10 days of receipt of purchase contract;
5.2.28.1.2 Delay in delivery beyond the specified period;
5.2.28.1.3 Serious discrepancy in functionality to be provided or the performance levels agreed upon, which have an impact on the functioning of the Bank. Inability of the Bidder to remedy the situation within 60 days from the date of pointing out the defects by the Bank. (60 days will be
construed as the notice period)
5.2.28.2 In addition to the cancellation of the contract, Bank reserves the right to appropriate the damages through encashment of Bid Security / Performance Guarantee given by the Bidder.
5.2.28.3 The Bank will reserve a right to re-negotiate the price and terms of the entire contract with the Bidder at more favourable terms in case such terms are offered in the industry at that time for projects of similar and comparable size, scope and quality.
The Bank shall have the option of purchasing the equipment from third-party suppliers, in case such equipment is available at a lower price and the Bidder’s offer does not match such lower price. Notwithstanding the foregoing, the Bidder shall continue to have the same obligations as contained in this RFP in relation to such equipment procured from third-party suppliers. As aforesaid the Bank would procure the equipment from the third party only in the event that the equipment was available at more favorable terms in the industry, and secondly, The Equipment procured here from third parties is functionally similar, so that the Bidder can maintain such equipment.
The modalities under this right to re-negotiate /re-procure shall be finalized at the time of contract finalization.
5.2.28.4 Notwithstanding the existence of a dispute, and/or the commencement of arbitration proceedings, the Bidder will be expected to continue the warranty/AMC/ATS services. The Bank shall have the sole and absolute discretion to decide whether proper reverse transition mechanism over a period of 6 to 12 months, has been complied with. In the event of the conflict not being resolved, the conflict will be resolved through Arbitration.
The Bank and the Bidder shall together prepare the Reverse Transition Plan. However, the Bank shall have the sole discretion to ascertain whether such Plan has been complied with.
Reverse Transition mechanism would typically include service and tasks that are required to be performed / rendered by the Bidder to the Bank or its designee to ensure smooth handover and transitioning of Bank’s deliverables, maintenance and facility management.

5.2.29 Corrupt and Fraudulent Practices

As per Central Vigilance Commission (CVC) directives, it is required that Bidders / Suppliers /Contractors observe the highest standard of ethics during the procurement and execution of such contracts in pursuance of this policy:
“Corrupt Practice” means the offering, giving, receiving or soliciting of anything of values to influence the action of an official in the procurement process or in contract execution AND “Fraudulent Practice” means a misrepresentation of facts in order to influence a procurement process or the execution of contract to the detriment of the Bank and includes collusive practice among Bidders (prior to or after offer submission) designed to establish offer prices at artificial non-competitive levels and to deprive the Bank of the benefits of free and open competition. The Bank reserves the right to reject a proposal for award if it determines that the Bidder recommended for award has engaged in corrupt or fraudulent practices in competing

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

5.2.30 Waiver

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

5.2.31 Violation of terms

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

5.2.32 Visitorial Rights

The Bank reserves the right to visit any of the Bidder’s premises without prior notice to ensure that data provided by the Bank is not misused.

5.2.33 Addition/Deletion of Qualified Offerings

Both parties agree that the intent of this tender is to establish an initial set of service offerings. The Bank recognizes that, as the use of these services expands, it is possible that additional services and / or service categories will be needed. In addition, the Bank recognizes that from time to time Proposed solution equipment and related products that are provided as part of Bidder services will be upgraded or replaced as technology evolve. Replacement and / or supplemental hardware and software products that meet or exceed the minimum proposal requirements may be added with the prior approval of the Bank. For this purpose, a Change Order Procedure will be followed. Bank may request a change order in the event of actual or anticipated change(s) to the agreed scope of work, services, deliverables and schedules. The Bidder shall prepare a change order reflecting the actual or anticipated change(s) including the impact on deliverables schedule. The Bidder shall carry out such services as required by the Bank at mutually agreed terms and conditions.

The Bidder shall agree that the price for incremental offering cannot exceed the original proposed cost and the Bank reserves the right to re-negotiate the price. At the unit rates provided for TCO calculations the bank has the right to order as much as it wants at those rates.

The Bidder shall agree to submit the request to add new services or service categories on its letterhead signed by a representative authorized to bind the organization.

The Bank is under no obligation to honor such requests to add service categories or amend this contract.

As a method for reviewing Bidder services and Bank requirements, the Bank will sponsor regular reviews to allow an exchange of requirements and opportunities.

All quantities mentioned in this RFP are indicative. The quantities of components to be procured as part of this tender can be varied by the Bank. This also includes the right to modify the number of branches, extension counters, offices, training centres etc.

5.2.34 Termination

1. Bank shall be entitled to terminate the agreement with the bidder at any time by giving Thirty (30) days prior written notice to the bidder.
2. Bank shall be entitled to terminate the agreement at any time by giving notice if:
    a. The Bank shall be entitled to terminate the Agreement at any time by giving at least 15 days notice to the Bidder
    b. The bidder breaches its obligations under the tender document or the subsequent agreement and if the breach is not cured within 30 days from the date of notice.
    c. The bidder (i) has a winding up order made against it; or (ii) has a receiver appointed over all or substantial assets; or (iii) is or becomes unable to pay its debts as they become due; or (iv) enters into any arrangement or composition with or for the benefit of its creditors; or (v) passes a resolution for its voluntary winding up or dissolution or if it is dissolved.
3. The bidder shall have right to terminate only in the event of winding up of Bank.

5.2.35 Effect of termination

5.2.35.1 The Bidder agrees that it shall not be relieved of its obligations under the reverse transition mechanism notwithstanding the termination of the assignment. Reverse Transition mechanism would typically include service and tasks that are required to be performed / rendered by the Bidder to the Bank or its designee to ensure smooth handover and transitioning of Bank’s deliverables and maintenance. The reverse transition will be for the period of 3 months post the notice period. Same terms (including payment terms) which were applicable during the term of the contract shall be applicable for reverse transition services

5.2.35.2 The Bidder agrees that after completion of the Term or upon earlier termination of the assignment the Bidder shall, if required by the Bank, continue to provide warranty/AMC services to the Bank at no less favorable terms than those contained in this RFP. In case the bank wants to continue with the Bidder's services after the completion of this contract then the Bidder shall offer the same or better terms to the bank. Unless mutually agreed, the rates shall remain firm.

5.2.35.3 The Bank shall make such prorated payment for services rendered by the Bidder and accepted by the Bank at the sole discretion of the Bank in the event of termination, provided that the Bidder is in compliance with its obligations till such date. However, no payment for “costs incurred, or irrevocably committed to, up to the effective date of such termination” will be admissible. There shall be no termination compensation payable to the Bidder.

5.2.35.4 Termination shall not absolve the liability of the Bank to make payments of undisputed amounts to not affect any accrued rights or liabilities or either party nor the coming into force or continuation in force of any provision hereof which is expressly intended to come into force or continue in force on or after such termination. the Bidder for services rendered till the effective date of termination. Termination shall be without prejudice to any other rights or remedies a party may be entitled to hereunder or at law and shall not affect any accrued rights or liabilities or either party nor the coming into force or continuation in force of any provision hereof which is expressly intended to come into force or continue in force on or after such termination.

5.2.36 Severability

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

ii. In the event any court or other government authority shall determine any provisions in this agreement is no amended so that it is enforceable to the fullest extent permissible under the laws and public policies of the jurisdiction in which enforcement is sought and affords the parties the same basic rights and obligations and has the same economic effect as prior to amendment.

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

5.2.37 Intellectual Property Rights

All Intellectual Property Rights in the deliverables (excluding Pre-existing Material or third party software, which shall be dealt with in accordance with the terms of any license agreement relating to that software) shall be owned by Bank. In the event that any of the deliverables or work product do not qualify as works made for hire, the bidder hereby assigns to Bank, all rights, title and interest in and to the deliverables or work product and all Intellectual Property Rights therein.

Notwithstanding the above, any intellectual property developed by a Party that is a derivative work of any pre-existing materials will be treated the same as pre-existing material and the developer of the derivative work will assign all right and title in and to the derivative work to the owner of the pre-existing material.

Residuals. The term "Residuals" shall mean information and knowledge in intangible form, which is retained in the memory of personnel who have had access to such information or knowledge while providing Services, including concepts, know-how, and techniques. There is no restriction on the use of the residual knowledge by personnel upon completion of their assignment with the Bank.

Other than as agreed hereinabove, nothing herein shall cause or imply any sale, license (except as expressly provided herein), or transfer of proprietary rights of or in any software or products (including third party) from one party to the other party with respect to work product, Deliverables or Services agreed under this Agreement.

5.2.38 Change Management

Changes to business applications, IT components and facilities should be managed by change management processes to ensure integrity of any changes.

All the IT components proposed under the RFP (such as- application software, middleware etc.) should be periodically patched for all types of patches, such as - security patches, system patches etc. Emergency patches should also be applied immediately as per regulatory and other agencies directions etc. If any proposed software becomes End of support/ End of life during the warranty/ AMC/ ATS period, the same will be replaced by the next version of software without any cost to the Bank. Also, software replacements are done in a planned manner to ensure that no downtime is required on this account.

5.2.39 Compliance with All Applicable Laws

The bidder shall undertake to observe, adhere to, abide by, comply with and notify Bank about all laws in force or as are or as made applicable in future, pertaining to or applicable to them, their business, their employees or their obligations towards them and all purposes of this tender and shall indemnify, keep indemnified, hold harmless, defend and protect Bank and its employees/officers/staff/ personnel/representatives/agents from any failure or omission on its part to do so and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from.

Compliance in obtaining approvals/permissions/licenses: The bidder shall promptly and timely obtain all such consents, permissions, approvals, licenses, etc., as may be necessary or required for any of the purposes of this project or for the conduct of their own business under any applicable Law, Government Regulation/Guidelines and shall keep the same valid and in force during the term of the project, and in the event of any failure or omission to do so, shall indemnify, keep indemnified, hold harmless, defend, protect and fully compensate the Bank and its employees/ officers/ staff/ personnel/ representatives/agents from and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from and the Bank will give notice of any such claim or demand of liability within reasonable time to the bidder.

This indemnification is only a remedy for Bank. The bidder is not absolved from its responsibility of complying with the statutory obligations as specified above. Indemnity would be limited to court awarded damages and shall exclude indirect, consequential and incidental damages. However, indemnity would cover damages, loss or liabilities suffered by Bank arising out of claims made by its customers and/or regulatory authorities.

This RFP shall be construed and interpreted in accordance with and governed by the laws of India, and the courts at Pune shall have exclusive jurisdiction over matters arising out of or relating to this RFP.

5.2.40 Data Privacy

The successful bidder must comply with proposed Data privacy bill.

5.2.41 GIGW Compliant

All the procurements should be GIGW (Guidelines for Indian Government Website) compliant for accessibility to physically disabled person. The procedure for making OCR based PDF files, W3C guidelines at http://www.w3.org/TR/WCAG20-TECHS/PDF7.html may be referred to.

5.2.42 Liquidated Damages

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

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

- Non-delivery of any component or other services mentioned in the order
- Non-delivery of supporting documentation
- Delivery/Availability, but no installation of the components and/or software
- Ill-integration
- System operational, but unsatisfactory to Bank

If the bidder fails to deliver any or all of the goods or perform the services within the time period(s) specified in the contract, Bank shall, without prejudice to its other remedies under the contract, deduct from the contract price, as liquidated damages, a sum equivalent to 0.50% of the complete contract amount until actual delivery or performance, per week or part thereof (3 days will be treated as a week); and the maximum deduction is 10% of the contract price. Once the maximum is reached, Bank may consider termination of the contract.

Further, Bank also reserves the right to cancel the order and invoke Bank Guarantee/Performance. Guarantees in case of inordinate delays in the delivery/ installation of the equipment. Bank may provide a cure period of 30 days and thereafter foreclose the Bank guarantee without any notice. In the event of Bank agreeing to extend the date of delivery at the request of the successful bidder(s), it is a condition precedent that the validity of bank guarantee shall be extended by further period as required by Bank before the expiry of the original bank guarantee. Failure to do so will be treated as breach of contract. In such an event Bank, however, reserves its right to foreclose the Bank guarantee.

5.2.43 Service Continuity/ Contract Extension

Bidder recognizes that all services as mentioned in this RFP document are vital to Bank and bidder agrees to provide continued services rendered by vendor or its OEM partners till the renewal of the contract after the contract expiry or till any other alternate solution is implemented by the Bank.

The clause is also applicable in case of termination of the contract before the expiry. In case of termination of the contract before expiry, the vendor agrees to provide services as mentioned in this RFP document until alternate arrangement is made by the Bank or 6 months, whichever is earlier.

6. Evaluation Process

The competitive bids shall be submitted in three stages
Stage 1 – Eligibility criteria
Stage 2 – Technical Bid Evaluation Criteria
Stage 3 – Commercial Bid Evaluation Criteria

6.1 Eligibility Bid

Eligibility criterion for the Bidders to qualify this stage is clearly mentioned in **Annexure 5 – Eligibility Criteria Compliance** to this document. The Bidders who meet ALL these criteria would only qualify for the second stage of evaluation. The Bidder would need to provide supporting documents for eligibility proof. All the credentials of the Bidder necessarily need to be relevant to the Indian market, if specified otherwise.
The decision of the Bank shall be final and binding on all the Bidders to this document. The bank may accept or reject an offer without assigning any reason whatsoever.

6.2 Technical Evaluation criterion

Technical Proposals of only those bidders shall be evaluated who have satisfied the eligibility criteria bid. The scoring methodology for technical bid components is explained in the following paragraphs. The proposal submitted by the bidders shall, therefore, be evaluated on the following parameters:

1. Technical Requirements (TR)
2. Technical Presentation (TP)
3. Past Experience (PE)

The proposal submitted by the bidders shall, therefore, be evaluated on the following Criteria:

Sr. No	Parameter	Weightage	Maximum Score	Minimum Score
1	100% Compliance to Technical Requirements	-	-	-
2	Technical Presentation	40%	150	105
3	Past Experience	40%	150	105
4	Site Visit	20%	100	70
	Total	100%	400	280

Bank may seek clarifications from any or each of the bidder as a part of technical evaluation. All clarifications received within stipulated time shall be considered for evaluation. In case a clarification is not received within the stipulated time, then the respective technical parameter would be treated as non-compliant and decision to qualify/disqualify the bidder shall be accordingly taken by Bank.

Bidder should ensure that any non-compliance against Annexure 01-Technical Requirements may lead to disqualification. Proposed solution by the bidder should ensure 100% compliance for Security solution scoped under this RFP for technical scoring based on the defined technical requirements. Any breach of the minimum compliance requirement will lead to disqualification of the bid.

Bidders scoring at-least the minimum score in each clause as mentioned in the table above i.e. an overall minimum score of 280 marks or more and providing 100% compliance to Technical Requirements will be declared technically qualified.

In the event of no bidders qualifying, Bank at its discretion may choose to award the contract to the highest scoring bidder or waive criteria to select more than one bidder complied with most of the eligibility and technical criteria as prescribed by Bank.

Also Bank may, at its sole discretion, decide to seek more information from the bidders in order to normalize the bids. However, bidders will be notified separately, if such normalization exercise is resorted to.

Technical Requirements

Minimum technical requirements for Security solutions under this RFP are given in **Annexure 1**. All the requirements are mandatory.

Scoring for Overall Technical Presentation (TP)

All the eligible bidders along with their OEMs will be required to make presentations to supplement their bids, showcase overall solution proposed. Bank will schedule presentations and the time and location will be communicated to the bidders. Failure of the bidder to complete a scheduled presentation to Bank may result in rejection of the proposal.

Sr. No	Overall Technical Presentation	Max Score	Score
1	Presentation Introduction and Industry Insight	30	
2	Project Plan	20	
3	Solution Positioning	25	
4	Execution Methodology	30	
5	Timeline Adherence	25	
6	Project Governance and adherence to SLAs	20	
Total Max Score →		150	

Scoring for Past Experience (PE)

Bidder and OEM's should provide details of past experience in implementing security solution scoped under this RFP. Past experiences will be calculated for each solution separately. Past experience of Bidder/OEM shall be evaluated and the score obtained by the bidder shall be considered for evaluation as given in the **Annexure 17: Past Experience**. The bidder should provide the details of all the implementations in banks including details of scope of project, number of branches with breakup of the role and proof of implementation experience.

Sr. No.	Past Experience	Score	Max Score
A	**Implementation of Data Loss Prevention (DLP) Solution**		50
	Implemented or under implementation in 3 or more Govt. Sector/Scheduled Commercial Bank/PSU's in India	50	
	Implemented or under implementation in 2 or more Govt. Sector/Scheduled Commercial Bank/PSU's in India	40	
	Implemented or under implementation in 1 Govt. Sector/Scheduled Commercial Bank/PSU's in India	35	
B	**Implementation of Data Identification & Classification Tool (DICT)**		
	Implemented or under implementation in 3 or more Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI Sector in India	50	
	Implemented or under implementation in 2 or more Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI Sector in India	40	
	Implemented or under implementation in 1 Govt. Sector/Scheduled Commercial Bank/PSU's/BSFI Sector India	35	
C	**Implementation of Database Activity Monitoring(DAM) Solution**		50

Sr. No.	Past Experience	Score	Max Score
	Implemented or under implementation in 3 or more Govt. Sector/Scheduled Commercial Bank/PSU's in India	50	
	Implemented or under implementation in 2 or more Govt. Sector/Scheduled Commercial Bank/PSU's in India	40	
	Implemented or under implementation in 1 Govt. Sector/Scheduled Commercial Bank/PSU's in India	35	
D	**Implementation of Endpoint Encryption**		50
	Implemented or under implementation in 3 or more Govt. Sector/Scheduled Commercial Bank/PSU's in India	50	
	Implemented or under implementation in 2 or more Govt. Sector/Scheduled Commercial Bank/PSU's in India	40	
	Implemented or under implementation in 1 Govt. Sector/Scheduled Commercial Bank/PSU's in India	35	
E	**Implementation of Patch Management Solution**		50
	Implemented or under implementation in 3 or more Govt. Sector/Scheduled Commercial Bank/PSU's in India	50	
	Implemented or under implementation in 2 or more Govt. Sector/Scheduled Commercial Bank/PSU's in India	40	
	Implemented or under implementation in 1 Govt. Sector/Scheduled Commercial Bank/PSU's in India	35	
Total Max Score →			250

Scoring for Site Visit

Bank would carry out reference site visits and/ or telephonic feedback with the existing customers of the bidder/OEM. The inputs that have been received from the customer would be considered by the bank and this might not need any documentary evidence. This rating would be purely on the inputs (like satisfaction of the organization of the product, timeliness of implementation, promptness of support services etc.,) provided by the bidder/OEM's customers and score would be assigned to bidder.

The bank at its discretion may reject the proposal of the bidder without giving any reasons whatsoever, in case the responses received from the site visits are negative.

The bidder would be required to coordinate for such interactions. However, the bidder would not be allowed to be party to the discussion between the bank & the bidder/OEM's clients.

This will be a techno commercial evaluation and accordingly the Technical evaluation will have 70% weightage and commercial evaluation shall have 30% weightage.

6.3 Commercial Bid Evaluation

Only those bidders who have qualified after Stage 2 of Technical evaluation will be eligible for the commercial bid evaluation.

The commercial bid evaluation will be done through reverse auction. However to know the indicate price of the commercial bid, which would be evaluated based on a "Total Cost of Ownership" (TCO) basis. If any vendor fails to quote against any of the services sought by the Bank, it will be presumed by the Bank that the cost of such items is included in the overall cost and will not accept any plea or excuse from the vendors later and such services have to be provided to the Bank without any extra cost along with all other services.

The Indicative Commercial bids of only those bidders who qualify the technical evaluation shall be opened. Indicative Commercial bids of the other bidders shall not be opened and their Earnest Money Deposit shall be returned. The bidders will have to submit the Indicative Commercial bid in the format as specified in Annexure 10 Commercial Bill of Materials. The Bidder is expected to provide Total Cost of Ownership (TCO) for the purpose of commercial evaluation. TCO shall comprise the costs that Bidder shall charge to the Bank for the duration of the contract

The detailed procedure and Business rules for the Reverse auction is provided in Annexure 16: Guidelines, Terms & Conditions and Process Flow for E-Procurement Auction. The Reverse Auction will be conducted by the Bank’s authorized Reverse auction service provider; the details will be provided during the later stages of tendering process. Specific rules for this particular event viz., date and time, start price, bid decrement value, time allowed to confirm bid duration of event etc. shall be informed by the Bank, well before the event to the participating short listed bidders.

The Bank reserves the right to ‘call off’/ cancel the tender proceedings of Reverse Auction or cancel the Tender at any point of time.

The price decided by the bank will be taken as the starting bid of the Reverse Auction and NOT for deciding the L-1 status. The L-1 bidder will be decided only later through techno commercial Process, on finalization of prices on completion of the Reverse auction process.

Please note that, failure or refusal to offer the services/goods at the price committed through Reverse Auction shall result in forfeiture of the Bid Security Deposit to Bank.

This is not withstanding Bank's right to take any other action deemed fit, including claiming damages, ‘Black Listing’ the bidder from participating in future Tenders that would be floated by the Bank for a period found fit by the Bank, and also using the associates like IBA. The complete escalation matrix starting from the lowest till the highest level of hierarchy of the bidder has to be submitted.

Combined Techno Commercial Evaluation

Bids will be evaluated as per Combined Quality Cum Cost Based System. The Technical Bids will be allotted weightage of 70% while Commercial Bids will be allotted weightage of 30%.

The technical scores of the bidders who qualify technical evaluation shall not be disclosed to the qualified bidders.

Bidders should provide indicative price only as there will be a Reverse Auction

Post Reverse Auction, bidders need to submit the revised Commercial Bid in the format specified in Annexure 10 Commercial Bill of Materials. This needs to be done within 48 (forty-eight) hours of completion of Reverse Auction.

On completion of Reverse Auction process, technically qualified Bidder with the lowest Commercial Bid would be declared as CLOW.

The Technically Qualified Bidder with the highest technical score after scrutiny and normalization would be declared as THIGH

The techno-commercial score shall be calculated as follows:

Total Score = (CLOW / C)*0.3 + (T / THIGH)*0.70.

Here C and T are the commercial and technical scores of the respective bidders.

For example: In a techno commercial evaluation weightage for technical consideration is 70% and weightage for cost is 30%. Three vendors namely A, B and C participated in the bid process and their technical scores are as under:

A=60 (sixty), B=80 (eighty), C= 100 (hundred)

The quoted prices for Vendor are as under:

A= INR 8000 (eight thousand), B= INR 9000 (nine thousand), C= INR 10000 (ten thousand)

As the weightage for technical parameter and cost are 70% and 30% respectively, the final scores shall be calculated as under:

CLOW = 8000

THIGH = 100

A= (60/100)*0.7 + (8000/8000*0.3) = 0.72

B= (80/100)*0.7 + (8000/9000*0.3) = 0.827

C= (100/100)*0.7 + (8000/10000)*0.3 = 0.94

Hence, 'C' (being highest score) would be considered as the winner and would be named as successful Bidder.

In case of a tie of Total Score between two or more bidders, the Bid with higher technical score would be chosen as the successful Bidder.

Bank will notify the name of the Successful Bidder.

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

If there is a discrepancy between words and figures, the amount in words shall prevail

If there is a discrepancy between percentage and amount, the amount calculated as per the stipulated percentage basis shall prevail

If there is discrepancy between unit price and total price, the unit price shall prevail if there is a discrepancy in the total, the correct total shall be arrived at by Bank

In case the Bidder does not accept the correction of the errors as stated above, the bid shall be rejected.

7. Service Levels

Bank expects the bidder to adhere to the Service Levels described in this document. Service Levels will include Availability measurements and Performance parameters. Bank requires the bidder to provide reports for all availability and performance parameters and a log of all issues that have been raised and closed / pending closure by the bidder. The frequency of these reports should be monthly and apart from reports on each availability and performance measurement parameter mentioned below, reporting should also include the following:

- Endpoint Compliance
- Problem Trends
- Call Resolution Time

Notwithstanding anything contained above, no such penalty will be chargeable on the Vendor under the above clauses for the inability occasioned, if such inability is due to reasons entirely attributable to the Bank.

Availability measurements and monitoring of Performance parameters would be on a monthly basis for the purpose of Service Level reporting.

Payments to the Bidder are linked to the compliance with the SLA metrics. During the contract period, it is envisaged that there could be changes to the SLAs, in terms of addition, alteration or deletion of certain parameters, based on mutual consent of both the parties i.e. Bank and Bidder.

The Bidder shall monitor and maintain the stated service levels to provide quality service. Bidder to use automated tools to provide the SLA Reports. Bidder to provide access to the Bank or its designated personnel to the tools used for SLA monitoring.

The successful bidder shall not be penalized for those service level breaches that occur due to any reason (beyond the control of the successful bidder). Bank will leverage the effort of the existing System Integrator for the EMS tool configuration for the bidder's proposed solution and its SLA measurement. The existing System Integrator of Bank will configure the operational parameters in the tool and define the threshold for Service level as defined in this document for reporting purpose. The basis of availability will solely be determined by the reports output from the EMS tool and the system generated reports. All the SLA will be measured considering dependency of any other third party assets, which has contributed to the breach.

Bank shall reserve the right to perform root cause analysis (RCA) by its internal team(s) or engage external parties to perform the same. The successful bidder shall cooperate with the team performing the procedures. Decision taken by bank for RCA performed shall be final.

Definitions

1. "Availability" means the time for which the services and facilities are available for conducting operations on the system including application and associated infrastructure.

Availability is defined as (%) = $\frac{\underline{\text{(Operation Hours – Downtime)}}}{\text{(Operation Hours)}}$ x 100%

2. The business hours are 8AM to 8PM on any calendar day the Bank's branch is operational. Vendor however recognizes the fact that the branches will require to work beyond the business hours on need basis.

3. All the infrastructure of Data Center, Disaster Recovery site, Offices/Branches will be supported on 24x7 basis.

4. The "Operation Hours" for a given time frame are calculated after deducting the planned downtime from "Operation Hours". The Operation Hours will be taken on 24x7 basis, for the purpose of meeting the Service Level requirements i.e. availability and performance measurements both.

5. "Downtime" is the actual duration for which the system was not able to Service Bank, due to System or Infrastructure failure as defined by the Bank and agreed by the Bidder.

6. “Scheduled Maintenance Time” shall mean the time that the System is not in service due to a scheduled activity as defined in this SLA. The scheduled maintenance time would not be during business hours. Further, scheduled maintenance time is planned downtime with the prior permission of the Bank

7. “Incident” refers to any event / abnormalities in the functioning of any of IT Equipment / Services that may lead to disruption in normal operations of the Data Centre, System or Application services.

Severity Levels:

Severity Definition during Live operations due to Infrastructure/Functional issues of the proposed solution, the SLA’s will be applicable post go-live of Proposed Solutions at DC, DRC, Branches and other Bank Offices.

Description: Time taken to resolve the reported problem Severity is defined as:

Level	**Function/Technology**
Severity 1	i Such class of errors will include problems, which prevent users from making operational use of solution. ii Security Incidents iii No work-around or manual process available iv Financial impact on Bank v Infrastructure related to providing solution to the Bank comprising of but not limited to the following: a. Proposed Solution Tools / Application Servers b. Proposed Solution Database Servers / Appliance c. Proposed Solution servers/appliances d. Network components, if any proposed by the bidder
Severity 2	i Any incident which is not classified as “Severity 1” for which an acceptable workaround has been provided by the Bidder or; ii Any problem due to which the Severity 2 infrastructure of the proposed solution is not available to the Bank or does not perform according to the defined performance and query processing parameters required as per the RFP or; iii Users face severe functional restrictions in the application irrespective of the cause. iv Key business infrastructure, systems and support services comprising of but not limited to the following: a. Solution Test & Development and Training Infrastructure and Application

Level	Function/Technology
	b. Infrastructure for providing access of dashboards, scorecards, etc.
Severity 3	i Any incident which is not classified as “Severity 2” for which an acceptable workaround has been provided by the Bidder; ii Moderate functional restrictions in the application irrespective of the cause. Has a convenient and readily available workaround. iii No impact on processing of normal business activities iv Equipment/system/Applications issues and has no impact on the normal operations/day-today working. v All other residuary proposed solution Infrastructure not defined in “Severity 1” and “Severity 2”

During the term of the contract, the bidder will maintain the equipment in perfect working order and condition and for this purpose will provide the following repairs and maintenance services.

Performance Measurement:

Service Area	Expected Output	Service Levels
Hardware Utilization	Hardware utilization should not exceed 70%	0.5% of Annual Subscription Cost for every 1% of deviation from the Minimum service Level (Minimum service level 99%)
Storage Utilization	Storage utilization should not exceed 90%	0.5% of Annual Subscription Cost for every 1% of deviation from the Minimum service Level (Minimum service level 99%)
Downtime for servicing	Each planned downtime for hardware, database and operating system servicing etc. (up gradation, bug fixing, patch uploads, regular maintenance etc.), attributable to the Bidder, will not be more than 4 hours. This activity will not be carried out during 9 AM to 9 PM. However, activities which require more than 4 hours or required to be carried out	Penalty of INR 10,000/- for every 30 minutes of delay above the scheduled/permissible window (Minimum service level 100% per instance)

Service Area	Expected Output	Service Levels
	during business hours will be scheduled in consultation with Bank	
Endpoint Compliance	All the identified endpoints in the Bank will be updated with the latest agent softwares/packages and it will be reporting to the centralized console on defined polling intervals.	Banks expects 95% compliance on monthly basis in this regard. Non-compliance of this will attract penalty of 5% of Annual Subscription Cost
Alert Management	Security solution shall be generating Alert within 15 minutes from occurrence of event. Solution shall be logging ticket for each alert generated within 5 minutes from alert notification	1% of the annual billing payment after discovery of the performance lacunae per week thereafter, till the problem is resolved
Disaster Recovery Site Availability	Business operations to resume from Disaster Recovery Site within 120 (RTO)minutes of the Data Centre failing	INR 5000 for every 10 Minutes of delay above the defined RTO for the reasons solely attributable to the bidder (minimum service level 100 % per instance)
Report and Dashboard	Periodic reports to be provided to Bank	• Weekly Reports: By 11:00 AM, Monday • Monthly Reports: 10th of each month • Delay in reporting by more than 3 days for both weekly and monthly reports shall incur a penalty of 2%
Continual Improvement	The Bidder is expected to improve the operations on an on-going basis The Bidder is expected to provide a quarterly report of the new improvements suggested, action plans, and the status of these Improvements to the Bank. Improvement areas could include: process changes/ training resulting in efficiency/ Service Level improvement, new correlation rules to identify threat patterns etc.	Quarterly reports need to be provided by the 10th day of each quarter beginning. Delay in providing quarterly reports shall lead to 2% of the Annual Subscription Cost.
Periodic Review	The project sponsor or locational delegate from the Bidder is expected to conduct a monthly review meeting with Bank officials resulting in a report covering details about current solution Service Levels, status of 0perations, key security breaches	Monthly meeting for next five years to be conducted on the 5th (tentatively) of each month during the operations phase. A delay of more than three days will incur a penalty of 1% of Annual Subscription Cost.

Service Area	Expected Output	Service Levels
	and new attacks identified, issues and challenges etc.	
Security solution management – Version / Release/Upgrades / patches	Bidder to inform Bank team and ensure that entire stack of solution – software, Operating system, Database etc. are updated with latest firmware, patches, upgrades, release, version, etc. as per the Bank policy.	• Penalty of 2% for every fortnight for not informing of the Bank of latest versions/release/upgrades/patch for **Solution** upon its release**.** • Penalty of 2% for every week for not informing of critical security patches of solution components. • Penalty of 2% for every week of delayed updating/patching beyond mutually agreed upon time schedule for any component of solution once notified by the Bank.
Audit of Security Solution	The security Solution infrastructure may be subjected to audit from Bank and/or third party	• Audit observations to be closed in mutually agreed timeframe. • Penalty of 2% for each week of delay in implementation of critical and important observations. Penalty of 1% for each repeated observations
Manpower services	Bidder to provide experienced and certified manpower at Primary site as per RFP. Any resource absence bidder should provide temporary replacement. Any lacuna will attract penalty	Penalty for resource absence shall be as follows :- L3 Absence - Rs3000/- per day L2 Absence- Rs2000/- per day and L1 absence Rs1000/- per day. Any resource to be relieved from project should give a three month prior notice to the bank. If resource leaves before prior notice of three months , resource will be marked absent and a penalty per day for remaining period will be levied.
Modification (Customization /	Any functional requirement (Change Request), after completion of sign-off formalities, will be delivered in UAT within mutually agreed timeline.	In case of delay, INR 5000 per day would be levied as a penalty for every instance of deviation

Service Area	Expected Output	Service Levels
Enhancements)resolution	However, delivery of Regulatory and Statutory requirements should be based on timeline mentioned by the respective Regulatory and Statutory authorities. For large/complex requirements; the priority and the time lines will be mutually discussed and agreed upon.	

<u>Note:</u> Penalty amount/percentage referred here will be deducted from Annual Subscription Cost wherever not specified.

7.1 Problem Management and Escalation Procedures

An escalation matrix would be applicable for the issues reported. Bidder has to propose an escalation matrix as a part of the Technical Proposal.

7.2 Penalty and non-adherence to the SLA

S.No	Level of uptime per month for Proposed Solutions	Penalty Charges
1	99.90% and Above	NIL
2	99.00% and above but below 99.90%	1% of Total of Annual Solution Subscription Cost and Facility Management Cost for Solution.
3	98.00% and above but below 99.00%	5% of Total of Annual Solution Subscription Cost and Facility Management Cost for Solution..
4	97.00% and above but below 98.00%	10% of Total of Annual Solution Subscription Cost and Facility Management Cost for Solution.
5	Below 97.00%	No payment and Bank also reserve the right to terminate the contract.

i Further if the number of downtime instances during a month exceeds 3 times, an additional 0.50% downtime will be reduced from uptime and the penalty will be calculated accordingly
ii If a breach occurs even after a proper (DLP/DICT & DAM) policy in solution is in place, a penalty of Rs.5000 /- per event will be deducted or the loss due to the breach whichever is higher.
iii The right to levy the penalty is in addition to and without prejudice to other rights / remedies available to the Bank such as termination of contract, invoking performance guarantee and recovery of amount paid etc.

Penalty shall be charged for every non-conformance with the service response and resolution time table as specified below:

Issue Classification	For All Periods (Post Go-Live)		Penalty
	Response Time	Resolution Time	
Severity 1	30 minutes	6 hours	5% of the Quarterly Payment

Issue Classification	**For All Periods (Post Go-Live)** **Response Time**	**Resolution Time**	**Penalty**
Severity 2	60 minutes	16 Bank Business Hours	2% of the Quarterly Payment
Severity 3	120 minutes	24 Bank Business Hours	1% of the Quarterly Payment

Bank reserves the right to recover the penalty from any payment to be made under this contract. The penalty would be deducted from the quarterly payouts and the cap on quarterly penalty will be 15% of the quarterly payout. The overall cap on penalty will be 10% of the total contract value.

7.3 Penalties for delayed implementation

1) The successful bidder must strictly adhere to the delivery dates or lead times identified in its proposal. Failure to meet these delivery dates, unless it is due to reasons entirely attributable to Bank, may constitute a material breach of the bidder’s performance. As a deterrent for delays during implementation, Bank may levy penalties for delays attributable to the successful bidder. Bank will ensure that the site for such installations in the standard IT DC specifications with availability of space, cooling and power for carrying out the rightful delivery, installation of the assets. The reasons like non-familiarity with the site conditions and/ or existing IT infrastructure will not be considered as a reason for delay
2) A cap of 10% of effected Product / Service line item value would be applicable as penalties for delays in meeting milestones
3) One percent of the total product fees would be levied as a penalty for every one week delay as per delivery timelines per product / service
4) Service Level shall be measured after a stabilization period/Go Live Date of 30 days from effective date of contractual obligation and continuously improved during the interim period till implementation of the services is over. The penalties shall be applicable on these service levels post 60 days of the completion of the implementation period for first pilot location
5) Service Levels shall be reviewed at least once every month during the period of contract and may be added/ deleted/ changed by Bank as a result of such review or any new business/ IT Services requirements

For a delay of more than 6 weeks in implementation, Bank will have the option of looking at more severe options like invoking the EMD/ PBG or cancelling the awarded contract.

7.4 Cap on Penalties

Overall cap for penalties including liquidated damages will be 10% of effected Product / Service line item value. Thereafter, the contract may be cancelled and amount paid, if any, will be recovered. Penalties on delay will be applicable when the delay is not attributable to Bank.

7.5 Overall Liability of the Bidder

The bidder's aggregate liability in connection with obligations undertaken as a part of the project regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), shall be at actuals and limited to the TCO. The bidder's liability in case of claims against Bank resulting from willful misconduct or gross negligence of the bidder, its employees and subcontractors or from infringement of patents, trademarks, copyrights or such other intellectual property rights, breach of confidentiality, or violation of any legal, regulatory, statutory obligations shall be unlimited.

8. Payment Terms

The Bidder must accept the payment terms proposed by the Bank. The financial offer submitted by the Bidder must be in conformity with the payment terms proposed by the Bank. Any deviation from the proposed payment terms would not be accepted. The Bank shall have the right to withhold any payment due to the Bidder, in case of delays or defaults on the part of the Bidder.

Such withholding of payment shall not amount to a default on the part of the Bank.

The scope of work is divided in different areas and the payment would be linked to delivery and acceptance of each area as explained below:

Subscription Cost

- Solution Subscription Cost would be payable on yearly basis in advance after sign-off the solution.

Hardware Cost

- 80% of the delivered Proposed solution equipment cost would be payable on successful post-delivery inspection of the respective Proposed solution equipment.

- 20% of the delivered equipment cost would be payable after sign-off of the solution.

Installation Costs:

- 100% of the Installation cost would be payable after installation of the respective proposed solution and installation report signoffs, if Performance Bank Guarantee is submitted.

Training Costs:

- 100% of the training cost would be payable after completion of all the trainings and submission of the training feedback from the people attending the training.

Facilities Management and other OEM Services Costs:

- The annual amount to be paid towards People deployment would be divided into 4 equal instalments, to be paid quarterly at the end of each quarter

- OEM Services Costs – ONE TIME; 100% of the cost would be payable after the submission of the report and report signoff.

- OEM Services Costs – Recurring; The OEM services recurring cost would be paid quarterly in arrears.

  Bidder's failure to deliver all required components of a fully functional system (pertaining to the scope of the project) within the stipulated time schedule or by the date extended by the Bank, unless such failure is due to reasons entirely attributable to the Bank, it will be a breach of contract. In such case, the Bank would be entitled to charge a penalty, as specified in Clause 5.2.14.

9 Response to RFP

The submission needs to be made at the address given below as per the schedule mentioned in clause Schedule of events in "Invitation to tenders". All envelopes shall be securely sealed and stamped. The authorized signatories of the Bidder shall initial on all pages of the technical and commercial proposals. Bidder need to ensure that the minimum required details are submitted.

General Manager (IT),
Bank of Maharashtra
Information Technology,
Head Office,
1501, Lokmangal, Shivaji Nagar,
Pune - 411005
The competitive bids shall be submitted in three parts viz.
1. Eligibility Evaluation
2. Technical offer
3. Commercial offer

Eligibility and Technical Bids shall be submitted in separate sealed sub-envelopes super scribing
"ELIGIBILITY BID FOR BANK OF MAHARASHTRA – **SUPPLY, IMPLEMENTATION & MAINTENANCE OF DLP, DICT, DAM, EE & PMS** TENDER REFERENCE NO._____ SUBMITTED BY M/S….. ON…..AT PUNE, DUE DATE _______"
on top of the sub-envelope containing the Eligibility bid
"TECHNICAL BID FOR BANK OF MAHARASHTRA – **SUPPLY, IMPLEMENTATION & MAINTENANCE OF DLP, DICT, DAM, EE & PMS** TENDER REFERENCE
NO._____ SUBMITTED BY M/s….. ON…..AT PUNE, DUE DATE ________ " on top of the subenvelope
containing the technical bid.
These two separate sealed sub-envelopes shall be put together in another sealed master envelope super
scribing BID for BANK OF MAHARASHTRA **SUPPLY, IMPLEMENTATION & MAINTENANCE OF DLP, DICT, DAM, EE & PMS** TENDER REFERENCE NO._____
SUBMITTED BY ….. ON…....AT PUNE, DUE DATE ________".

The response shall be organized and submitted in the following manner:

9.1 Eligibility Bid

1. Duly filled up Annexure 5 – Eligibility Criteria Compliance
2. Supporting credential letters or copies of documentation from clients or system integrators certifying compliance

9.2 Technical Offer

1. Table of Contents (list of documents enclosed by the Bidders)
2. 1 copy of the technical proposal with pages properly numbered. The technical proposal shall be bound in such a way that the clauses of the proposal could be removed and separated easily;

3. Annexure 10 - A copy of the entire Bill of Materials after masking the prices with XXX.

4. 1 copy of the masked price bid (masked price bid is a copy of the price bid without any prices. Please note that the masked price bid shall be an exact reflection of the indicative commercial bid submitted by the Bidder as part of the indicative commercial offer except that the Masked price bid shall not contain any financial information.)

5. 1 compact disk (CD) containing the soft copy of technical proposal shall be provided

9.3 Commercial Bid

1. 1 hard copy of the commercial proposal (Refer Annexure 10 – Bill of Material details for format).

2. 1 compact disk (CD) containing the soft copy of the commercial proposal (Refer Annexure 10 – Bill of Material details, for format)

Please note that if any envelope is found to contain technical and commercial offer in a single envelope, then that offer will be rejected outright.

The Bidder shall certify that the contents of the CD's are the same as that provided by way of hard copy. In the event of a discrepancy, details provided in the hard copy will be true.

All the pages of the proposal including annexure, appendices and documentary proofs shall be numbered and be signed by the authorized signatory

Copy of the RFP duly putting the seal and signature on all the pages of the document for having noted the contents and testifying conformance to the terms and conditions set out therein shall also be enclosed in the Master Envelope.

The proposal shall be prepared in English in MS Word / Excel / Power point format. The email address and phone / fax numbers of the Bidder shall also be indicated on sealed envelopes.

Bidder shall submit two separate demand drafts/banker's cheques / pay orders drawn in favor of Bank of Maharashtra payable at PUNE towards Application Money and Bid security as stated in clause 1 of this document.

Paper copies of RFP response shall be submitted along with Demand draft / Banker's cheque / Pay order for application money (which shall be non- refundable and bid security deposit and electronic copy (Microsoft word and Excel on CD ROM) of technical bid submissions must be submitted to the bank at the following address:

General Manager (IT),
Bank of Maharashtra
Information Technology,

Head Office,
1501, Lokmangal, Shivaji Nagar,
Pune – 411005.
The sealed bid envelopes as mentioned above shall be dropped in the Tender Box kept in the IT, Department. The following officials shall be available for any assistance.
Mr Rajkiran Lalam, Senior Manager-IT
Mr Prashant Chavan, Manager-IT
Mr Jeya Sakthi Velan, Manager-IT

Submission will be valid only if:

Copies of the RFP response documents are submitted as per defined clauses in Clause 9 and before the mentioned RFP closing date and time.

Submission is not by Fax transmission. Only one Submission of response to RFP by each service provider will be permitted.

In case of partnerships / consortium, only one submission is permitted through the lead service provider.

Last date for submission of the response to the tender document is mentioned in Clause 1 of this document.

All responses would be deemed to be irrevocable offers / proposals from the Bidder's and may if accepted by the Bank form part of the final contract between the Bank and the selected Bidder. Bidder is requested to attach a letter from an authorized signatory attesting the veracity of information provided in the responses (Annexure 6 – COVER TO).
Unsigned responses would be treated as incomplete and are liable to be rejected.

9.4 Contact Details for Responding to the Proposal

The bids (arranged as mentioned above) to be submitted, shall be addressed to General Manager (IT), Bank of Maharashtra, Information Technology, Head Office, 1501, Lokmangal, Shivaji Nagar, Pune – 411005 before the due date & time as per the schedule mentioned in clause Schedule of events in "Invitation to tenders" of RFP. The offer submitted anywhere else is liable to be rejected. The contact details of the Banks personnel are also provided in the same clause.

9.5 Proposal Format

The Bidder's proposal must effectively communicate their solution and be formatted in the specified formats in order for the Bank to assess the alternatives. Therefore, proposals must be submitted with the following clauses:

9.6 Technical Proposal Format

The technical offer shall be structured in the following sequence

a) Index

b) Covering letter as per Annexure 6 – Cover Letter

c) Bidder shall also provide the supporting document providing Company's authorization of its representative to bid, sign, and attend meetings.

d) Executive Summary

The Executive Summary shall be limited to a maximum of five pages and shall summarize the content of the response. The Executive Summary shall initially provide an overview of Bidder's organization and position with regards to Proposed solution equipment and professional services in Banking Sector. A summary of the Bidder's products and services that will be provided as a part of this procurement shall follow. A brief description of the unique qualifications of the Bidder. Information provided in the Executive Summary is to be presented in a clear and concise manner.

e) Delivery Schedule plan Detailed Work Plan (Project Plan) for all the equipment as mentioned in Clause 4 “Scope of Work” and Clause 2.3.1 “Project Timelines” of this document. A PERT chart providing the delivery plan and scheduled date of commencement of delivery and completion of the delivery shall also be provided;

f) Queries in the format as given in Annexure 8

h) Manufacturers’ Authorization letter in the format provided in Annexure 14 – Manufacturer Authorization from each OEM of whose the solution is being proposed by the bidder.

i) Annexure 22 – Resource Plan matrix

j) Annexure 4 - Conformity Letter

k) Annexure 3 - Conformity with Hardcopy Letter

l) Bill of Materials as per format provided in Annexure 10 - Bill of Materials (masked)

m) Bid Security Annexure 9 - Bid Security Form

10 Definitions & Reference

10.1 Working Day

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

10.2 Business hours

Business Hours for the purpose of service standards would be 8.00 am to 8.00 pm., on all working days for all the branch locations.

10.3 Restore to Service

Provides standard maintenance services including:

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

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

10.4 Obligations of the Bidder

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

a) Bidder shall assign personnel of appropriate qualifications and experience to perform the services in order to fulfill its obligations.

b) Bidder shall designate one of its personnel as the Project Manager, to interact with the Designated Customer Support Contact from the Bank for the purposes of getting approvals, progress report, discussing and resolving issues, arranging meetings, etc.

c) Bidder shall exercise requisite control and supervision over its personnel in the course of rendering the services and make best efforts to ensure that the services are rendered in a continuous and uninterrupted manner.

d) Bidder will have the right to withdraw its personnel, by replacing the persons with others having appropriate experience and skills at its own cost. Bidder shall seek necessary permission from the Bank 1 month in advance.

e) In the event that any person engaged/deputed/deployed for rendering services, is, either; No longer available by reason of resignation or termination or the like; or unable to render satisfactory services; or not acceptable to the Bank by reason of any misconduct or non-performance on the part of such person.

f) Bidder will use all reasonable endeavors to replace such individual promptly by another sufficiently skilled, qualified, and experienced with appropriate certifications personnel at its own cost. Bidder will in the discharge of its obligations use all reasonable endeavors to minimize changes in personnel.

g) Bidder will respect the confidentiality of all information given to it by the Bank and will not divulge such information to any third party or other units without the consent of the Bank.

11 Disclaimer

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

12. Annexures

Annexure 1: Technical and Functional Requirements for DLP, DICT, DAM, EE & PMS.

1.1 Technical and Functional Requirements for Data Loss/Leakage Prevention (DLP) Solution:

Sr. No	Technical Requirements (DLP)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
1	Proposed solution should have a comprehensive list of pre-defined policies and templates withover 1700+ patterns to identify and classify information pertaining to the Banking and Financial Institutions & in-line with the IT Act of India.		
2	All the policies should also reside on the agent and there must be synchronization of policies with central policy repository at regular time interval, which in turn offers full coverage of DLP when endpoint is on or off the Bank's network.		
3	Proposed should provide for dynamic application of policies and endpoint configurations based on agent properties, user or machine directory properties and conditions.		
4	Proposed solution should also monitor data downloads.		
5	Proposed solution should be able to monitor and protect data classifiers created in via the Fingerprinting of the structured and unstructured, it need to be synched to all the Network DLP channels and to Endpoint Channel.		
6	Proposed solution should be capable of Agent-based discovery of confidential data on Windows and Mac endpoints (desktops/laptops), including reporting on Access Control Lists (ACLs) for files that violates policy of the Bank.		
7	Proposed Solution should be threat-aware and the data protection should combine unmatched data loss prevention with Bank's Endpoint Antivirus Solution, defending against stealth data theft by malicious and dirty (suspicious or unknown) apps.		
8	Proposed solution should provide capabilities to identify data based on keywords or dictionaries and the solution should be able to enforce policies based on file types, size of files and the name of the file.		
9	Proposed solution should be able to detect encrypted and password protected files. The solution should be able to do full binary fingerprint of files and should be able to detect even if partial information gets leaks from fingerprinted files or folders. The solution should be able to recursively inspect the content of compressed archives		

Sr. No	Technical Requirements (DLP)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
10	Proposed solution should designate individual (or groups of) removable devices as trusted and create policy exceptions for those devices		
11	Proposed should Support running of server component of endpoint products in a VMware image		
12	The Endpoint DLP Solution must be able to encrypt data when business classified data is sent to removable media drives. The encryption solution can be built in or 3rd party solution needs to be factored to meet the requirement		
13	Proposed solution should detect ⏵ Patterns in binary file types and color maps for images. ⏵ keywords/patterns based on location (beginning/end) and proximity to each other within documents ⏵ Full Boolean expression for keywords and key phrases. ⏵ Pre-built dictionaries ⏵ wide range of sensitive data types (e.g., Aadhar, PAN, SSNs, CCNs, UID) ⏵ Patterns with respect to PCI-DSS policy template ⏵ classified Proprietary File types (types that are not predefined) and on file content not on file extensions. ⏵ fingerprints contents in an automated way where the user does not have to touch the files or import hashes ⏵ Fingerprinting task and pass on the same to all appliances (data in motion and rest) at once without the manual process from the user.		
14	Proposed solution should classify files as Encrypted based on statistical analysis of files.		
15	The solution should Support PrtSc blocking on endpoint when configurable list of specific application are running, no matter it is in the foreground or background. The actual PrtSc capture will also be submitted to the DLP system as forensic evidence.		
16	Proposed Solution should support the monitoring and blocking the printing activities to the Network or the Local Printer irrespective of Drivers used. Solution should support RAW printing mode as well.		
17	Proposed Solution should provide the data-labelling framework for the classification vendors like Bolden James, Titus, Microsoft AIP or other classification tool proposed by the Bidder for Auto Classification.		

Sr. No	Technical Requirements (DLP)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
18	The solution should have more than 60 pre-defined applications and multiple application groups and allow each application/application group to monitor operations like Cut/Copy, Paste, File Access and Screen Capture or Download. Also solution should have the capability to define the third party application.		
19	The solution should be able to define the policies for the inside and out of office endpoint machines.		
20	Proposed solution should be able to monitor data copied, printed and sent to removable media for structured and unstructured fingerprint policies even when disconnected from corporate network.		
21	Proposed solution should Support print screen blocking on endpoint when configurable list of specific application are running, no matter it is in the foreground or background. The actual print screen capture will also be submitted to the DLP system as forensic evidence.		
22	The solution should Provide “Cloud Storage Applications” group which monitor sensitive content accessed by these cloud storage application on the endpoint and prevent sensitive data from uploading to the cloud. For Example (Should support from day 1(Windows 10 and MAC OSX 10.13.6) -Amazon Cloud Drive, Box, Dropbox, Google Drive, SkyDrive, ICloud.		
23	Proposed solution should ▸ monitor/block data copied to removable storage devices (USB, Firewire, SD, Thunderbolt on MAC , MTP on Windows, eSATA and compact flash cards) ▸ Monitor/block data copied to CD/DVD ▸ Monitor/block corporate email via Microsoft Outlook. ▸ Monitor/block HTTP transmissions ▸ Monitor/block HTTPS transmissions via Microsoft Edge, Internet Explorer, Mozilla Firefox, Safari or Google Chrome ▸ Monitor/block FTP & SFTP transmissions ▸ Monitor/block or exclude detection (by printer name) of data sent to local or network printer ▸ Monitor/block data sent to a local or networked fax ▸ Monitor/block cut, copy or paste actions ▸ Monitor/block data copied to or from network file shares via Windows Explorer		

Sr. No	Technical Requirements (DLP)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
	▶ Monitor/block data copied to network file shares from MAC clients ▶ Monitor/block data copied through Conventional Remote Desktop Protocol (RDP), RDP through PIM Application & Dameware Mini Remote Control ▶ Monitor/block use of confidential data by defined applications, including unauthorized encryption tools, Instant Messaging programs and apps with proprietary protocols. Out-of-the-box coverage for Webex, LiveMeeting, Gotomeeting, Bluetooth and iTunes ▶ Monitor/blocks use of Lotus Notes 9.0 and above ▶ Monitor/blocks Microsoft Office 2013/2016 file formats for detection and application monitoring, including the default formats for Microsoft Access, Excel, OneNote, Outlook, PowerPoint, Project, Publisher, and Word. ▶ Monitor/block policy violations based on metadata ▶ Monitor/block —save as operations from Microsoft Office applications (Word, Excel, and PowerPoint) & Lotus Notes 9.0 and above to Box on Windows endpoints ▶ Monitor/block Save operations from Outlook (versions 2013 and 2016) using the Box for Office add-in		
24	Proposed solution should provide for multi-vendor support for Virtual Desktop Infrastructure architectures, covering monitor storage volumes, print and fax requests, clipboards, and network activity on the virtual desktops.		
25	Proposed Solution should have the ability to protect large volumes of data - entire database of customer records, large number of fingerprinted documents		
26	Proposed Solution should allow automatic movement or relocation of file, delete files during discovery and should display the original file location and policy match details for files found to violate policy		
27	Endpoint solution should support win 32 and 64 bit OS, Mac & Linux OS,Support wide variety of platforms(Below support from Day1):Windows 7, Windows 8.1, and 10, Windows server 2008 R2 and above, Mac OS X -10.11.X,10.12.x, Red Hat Linux/Cent OS , VDI (Citrix and VMWare)		
28	Proposed solution should be able to identify and block malicious activity like data thefts through files encrypted using non-standard algorithms.		

Sr. No	Technical Requirements (DLP)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
29	Proposed solution should have the ability to store and index the capture event data with appropriate metadata (date/time, user, protocol).		
30	Proposed Solution Should support large-scale storage capability such as SAN to hold metadata and raw data for investigators and regulators.		
31	Proposed solution should Index and retain all unfiltered files that are analyzed while scanning file servers, Desktops/laptops, Web and FTP/SFTP servers		
32	Proposed solution should conduct searches for content indexed during the following: i. Data-at-rest/motion/in-use based on keywords ii. Data-at-rest/motion/in-use based on document type iii. Data-at-rest/motion/in-use based on file owner, path, or age.		
33	Proposed Solution should be able to detect malicious dissemination, Password Protected and encrypted Files. Also detect the web uploads over the Dark Web sites.		
34	Proposed solution should support scanning of the database. Should support Oracle, MySQL, Microsoft SQL Server and IBM DB2.		
35	Proposed solution should support web-based file crawling HTTP, FTP, SFTP & HTTPS without having to install any software on servers to be scanned.		
36	Proposed solution should support Windows(CIFS), Samba on Unix, NFS without having to install any software on servers to be scanned.		
37	Proposed solution should Support multiple conditions by combining different data classifier, including Policy Template, Patter, RegEx, Keyword, Dictionary, Natural Language Policy (NL) as well as Fingerprinting. For example : i. ID# by policy template ii. CCN# by policy template iii. Name by fingerprinting iv. Address by fingerprinting		
	And then create a policy with multiple matching conditions including (i and ii) or (i and iii) or (i and iv)		
38	Proposed solution should be able to Configure and distribute action rules, including email notification, blocking, quarantining, redirection, and bouncing.		

Sr. No	Technical Requirements (DLP)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
39	Proposed solution should be able to detect, monitor & block the data from scanned documents as per the DLP policies either defined by the Bank or as pre-defined templates/policies/rules. Solution should have Optical Character Recognition (OCR) capability.		
40	Proposed solution should be able to Identify content using regular expressions, key words, hash functions, Document Fingerprint Signatures and pattern matching.		
41	Proposed solution should be able to Identify mass storage device by OEM/vendor specific identification numbers.		
42	Proposed Solution should be capable of storing the evidences generated against the DLP policy violations centrally as well as locally in encrypted form. Agents will be capable of synching the locally stored evidences with centralized location and it should be accessible from incident management console.		
43	Proposed solution should be capable to define monitoring filters for copy to network shares from Mac and Windows endpoints and from network shares to Windows local drives.		
44	Proposed solution should be capable to enable or disable specific channels based on the agent location.		
45	Proposed solution should enable Bank to classify newly created content, existing files, and emails in a DLP policy-driven or user-driven manner.		
46	Proposed solution should have ability to prevent printing of Microsoft Office documents if they contain sensitive information, regardless of whether a particular printing job does not include the sensitive portion.		
47	Proposed solution should provide an option of policy/rule override, which can be authorized to use an override code issued from the security administrator based on the end user's justification.		
48	The endpoint solution should Blocking of non-Windows CD/DVD burners, it should also Inspect and optionally block Explorer writes to WPD class devices. The endpoint solution should encrypt information copied to removable media. It Should support both Native and Portable Encryption and manage the Encryption and DLP policies from the same management Console.		

Sr. No	Technical Requirements (DLP)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
49	Proposed solution should support the multiple Endpoint Profile Creation between the different departments. Encryption Keys are also should be isolated between the different departments.		
50	Proposed solution should able to detect and Block the sensitive information uploads to Group of P2P software :- Bit torrent, µtorrent etc.,		
51	The DLP solution should consolidate small chunks of data leaks into a single incident		
52	Emails violating DLP policies should be quarantined with an automated email based workflow to remediates to take a single click actions like release or block without having to log into the DLP console		
53	The DLP Solution must provide visibility into Broken Business process. For ex:-if unsecured sensitive content is sent daily from several users to a business partner, the users are probably not aware that they are doing something wrong		
54	The Proposed DLP engine must performs a post-processing incident grouping step to avoid displaying related incidents in different cases. All incidents from the same user that have the same classification are combined into a group and DLP case card		
	POLICY MANAGEMENT		
55	Proposed Solution's Policy engine should allow Bank to set up different classification taxonomies and policies to be applied to designated users. Same policies should be deployed to both agentless and agent- based scans.		
56	The Policy management should include the following features and options: i. Selection of data type(s) and user group(s) using Active Directory. ii. Enabling exceptions for allowed users. iii. Flow direction to enforce on outbound or interdepartmental traffic. iv. Pre-defined policies and content data types.		
57	Proposed solution should be able to enforce policies while the endpoint system is disconnected from the Bank network and the endpoint agent should log all violations and reports into the central database when a connection to the Bank network is established.		

Sr. No	Technical Requirements (DLP)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
58	Proposed solution should be able to enforce different policies for desktops, servers and laptops.		
59	Proposed solution should be able to Identify content based on location and allow creation of policies based on Users and Groups.		
60	Proposed solution should enforce fingerprinting policy on both network and endpoint channel, even when the endpoint is off network by using Python, complex logic, rating and algorithm can be developed as a custom data classifier where customer can use in compound with any existing data classifier to identify sensitive data which is unique to the Bank.		
61	Proposed solution should have highly scalable architecture with centralized management that integrates with data loss prevention, Encryption and Identity Services.		
62	Proposed solution should have the ability to define a single set of policies based on content, sender/recipient, file characteristics and communications protocols once and deploy across all products.		
63	Proposed solution should have the ability to search across all captured data (not just incidents) on the network DLP system, then modify and test rules offline and implement the rules on live data thus reducing false positive.		
64	Proposed solution should provide a single policy framework for Network and Endpoint DLP.		
65	Proposed solution should provide ability to configure policies to detect, monitor and block on fingerprints and files from share/repository/date created etc.		
66	Proposed Solution should provide application of different agent configurations (covering different user actions, for example) to individual agents or groups of agents		
67	Proposed solution should provide directory based policies to selectively monitor downloads based on user, business units, or directory groups, specific groups of computers and specific groups of users.		
68	Proposed solution should provide for automatic tagging and watermarking all unstructured data, including emails, documents, and images according to Bank‘s policy.		
69	Proposed solution should provide Out of the Box Rule Sets.		

Sr. No	Technical Requirements (DLP)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
70	The Proposed DLP Solution must be GDPR and CCPA Compliant		
71	Proposed solution should provide pre-defined policies for identifying possible for identifying possible expression that are indicative of cyber bullying , self-destructive pattern or employee discontent , Mail to Self etc.,		
	AGENT MANAGEMENT		
72	Agent of Endpoint DLP should be supported on ▸ Windows Enterprise or Standard (64-bit) 2008 R2 and 2012 R2 ▸ Microsoft Windows Server 2016 Standard or Datacenter Edition (64-bit)		
	▸ Windows 7 Enterprise, Professional, Ultimate (32-bit & 64-bit) SP1 ▸ Windows 8.1 Enterprise, Pro PC operating system (64-bit) Unpatched, Update 1, Update 2, Update 3 ▸ Windows 10 Enterprise, Professional PC operating system (64-bit) Version 1709 & above. ▸ Apple macOS 10.12 (64-bit) and above.		
73	A fully functional and dedicated agent management console should be provided for the Endpoint administrator which should provide for agent troubleshooting and diagnostic tools designed for non-IT users		
74	Ability to centrally define or change Endpoint Agent uninstallation and management passwords		
75	Agent installed should have the capability to create the Bypass ID after validation by the administrator by generating the Passcode.		
76	Agent should be able to perform discovery only when the endpoint is connected to external power or Machine is Idle.		
77	Agent should be able to store both structured and unstructured fingerprints on the endpoint itself and should perform all analysis locally and not contact and network components to reduce WAN overheads.		
78	Agent should be deployed using a standard System management tools		
79	Agent should have capabilities to monitor applications and ensure unauthorized applications do not have access to sensitive files.		

Sr. No	Technical Requirements (DLP)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
80	Agent should have the ability to disable Print Screen / Shift Print Screen operations in supported Windows Operating Systems		
81	Agent should have the ability to Monitor and whitelist Windows Store applications		
82	Agent Should have the capability to containerize files to temporary storage- to prevent sensitive information from being written from an endpoint to a removable device—such as a USB flash drive, CD/DVD, or external hard disk		
83	Agent should have the capability to discover the Files that are modified between the specified Dates or Month Ago or Also for specific size to reduce the bandwidth and effective discovery.		
84	Agent should Integrate with Windows OS drivers and various applications to ensure stability, interoperability, and security.		
85	Agent should monitor and report last time an Agent received and applied new policies		
86	Agent should not appear in —Add/Remove Programs and System Tray, and obfuscated in Services and Task Manager		
87	Agent should provide for Centrally enable/disable the SPDY protocol on Internet Explorer and Firefox browsers		
88	Communications between agent and server should be encrypted and authenticated and Agent-Server authentication should be based on standard protocols (HTTPS/certificates)		
89	Proposed Solution should have an Option to require a password for agent uninstall		
90	Proposed Solution should have Load-balancer and firewall friendly architecture to support Agents-Server communicating over public networks		
91	Proposed Solution should have the ability to control Agent-Server connection interval and bandwidth throttle.		
92	Proposed Solution should have the ability to support up to 25,000 endpoint agents per server		
93	Proposed Solution should have the capability to Point agent(s) to different Endpoint Server at any time, and configure agent(s) to fail over to secondary server if primary is not available		

Sr. No	Technical Requirements (DLP)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
94	Proposed Solution should provide for Out-of-the-box agent tamper-proofing protection		
95	Proposed Solution should provide for targeted Agent deployment by AD groups or Windows groups		
96	Single agent should performs all the functions including endpoint scanning and monitoring/blocking data leaving the endpoint.		
97	Solution should have the capability to enable Bank to set caps on % of CPU and disk, and amount of bandwidth used by agent for minimal impact on endpoint and network		
98	The agent should Monitor content traversing across the endpoint by I/O channel (bus, Bluetooth, LPT, etc.) & Application Access.		
99	The agent should protect itself from unauthorized removal or service stoppage.		
100	The agent should stores incident-causing files in a cache until user reconnects to the Bank's network		
	SINGLE CENTRALIZED MANAGEMENT CONSOLE		
101	Configurations and control of all scanning should be possible from the single, centralized console		
102	Proposed solution should have centralized management and unified policy enforcement platform.		
103	Proposed solution should have mechanism to segregate and provide individual dasboard view and incident management console pertaining to the specific policy owner.		
104	Proposed Solution should provide for management of agent restart/shutdown, agent enable/disable, log retrieval, setting of logging levels, alerts, and configuration through central console.		
105	The central Management console should have a Built-in Agent health status dashboard		
106	The dashboard must display the number of cases in the designated period that fall above the risk score threshold that you've selected. Risk score thresholds must be customizable and instantly produce an report to prioritize the cases from high-to-low risk levels by leveraging analytics or machine learning technologies.		
107	The solution should also have a dashboard view designed for use by executives that can combine information from data in motion (network), data at rest (storage), and data at the endpoint (endpoint) in a single view		

Sr. No	Technical Requirements (DLP)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
108	The solution should check the health status of any managed appliance, including CPU utilization, disk utilization, and network throughput etc. and the same should be displayed on the dashboard.		
109	The solution should support the deployment of agent using the Central Management Console or common software deployment methods.		
	DATA SCANNING		
110	Agent-based scanning should enables parallel scanning of thousands of endpoints.		
111	Agents should report progress to a central location for up-to-date progress report while scans are running.		
112	Proposed solution should have Agentless and agent-based data scanning options.		
113	Proposed Solution should have the ability to failover a secondary Endpoint Server for endpoint discover scan.		
114	Proposed Solution should have the ability to quarantine confidential files locally (on endpoint) or to another network location.		
115	Proposed Solution should leave the "last accessed" attribute of scanned files unchanged so as not to disrupt enterprise backup processes.		
116	Proposed Solution should provide Configuration of incremental scans in which only new or changed files are scanned.		
117	Proposed Solution should provide for Filter scans based on file size, type, location, and operating system environment variables.		
118	Proposed Solution should provide for Option to configure scan timeout by specifying maximum overall duration or maximum idle period.		
119	Proposed Solution should provide for scan to run only when machine is idle, thus eliminating any adverse machine impact.		
120	Proposed Solution should Schedule automatically recurring scans and should have the capability to throttle and carry out Incremental scans to limit network bandwidth usage.		
121	Proposed solution should support incremental scanning during discovery to reduce volumes of data to be scanned.		
	END USER NOTIFICATIONS		
122	Automatic email notification should be sent to user and/or reporting authority upon the generation of an incident.		

Sr. No	Technical Requirements (DLP)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
123	Pop-up notification should have automatic ability to present itself in one of the languages based on underlying OS.		
124	Proposed Solution should have Option for endpoint user self-remediation (on-screen notification prompting user to confirm whether to continue or cancel confidential data transfer).		
125	Proposed Solution should have the ability to suggest or enforce classification and digital rights management protection for end users in real-time.		
126	Proposed solution should notify the end user of a policy violation using a customizable pop-up message with hyperlinks and fields for user justification and should capture content that violates a policy and store it in an evidence repository.		
	NETWORK DLP		
127	Proposed Solution should detect and prevent content getting posted or uploaded to specific websites, blogs, and forums accessed over HTTP, HTTPS. The solution should be able to enforce policies by URL's, domains or URL categories either natively or by integrated Web Security solution or by integrating with network DLP.		
128	Proposed Solution capture all TCP Protocols and protocol detection should be port agnostic. The solution should not discard any unidentified protocols and capture all traffic.		
129	Proposed Solution must have capability to integrate with 3rd party Proxy solution for content inspection using ICAP channel or must have DLP engine on OEM provided Proxy itself.		
130	Proposed Solution Should be able to capture all the data flowing outside of the network even if there is no policy configured to match the data. This data should be used later to do a search for after the fact incident so the the admin can do a forensic investigation.		
131	Proposed solution should be able to detect and block encrypted and password protected files without reading the encrypted content.		
132	Proposed Solution should be able to identify data leaked in the form unknown and known encrypted format like password protected word document.		

Sr. No	Technical Requirements (DLP)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
133	Proposed Solution should be able to identify malicious traffic pattern generated by Malware infected PC in order to prevent future data leakage by the malware.		
134	Proposed Solution should be able to monitor FTP traffic including fully correlating transferred control information and should be able to monitor IM traffic even if it's tunneled over HTTP protocol.		
135	Proposed Solution should Index and retain all documents and unfiltered network traffic that the network sensor analyzes.		
136	The proposed solution should conduct the following searches:		
	i. Any e-mail sent from or to email addresses ii. Any traffic sent from or to IP addresses or URLs iii. Any traffic sent across protocols or ports iv. Documents leaving the network based on document type.		
137	The solution should support the templates for detecting the Deep Web Urls- .i2P and .Onion , Encrypted attachments to competitors , Password Dissemination , User Traffic over time , Unknown Encrypted File Formats Detection.		
138	Proposed Solution should also able to monitor and block the File Uploads to the destinations that bypass the browser extensions such as Google Drive , Web.Whatsapp.com etc.,		
139	Proposed solution should be able to alert and notify sender, sender's manager and the policy owner whenever there is a policy violation, Different notification templates for different audience should be possible.		
140	Proposed solution should be able to block outbound emails sent via Outlook and Lotus Notes and can integrate with Network Email DLP with the single management console. Also natively monitors and block the internal emails shared between the different department.		
141	Proposed Solution should be able to detect and protect for the low volume data leaks over the Network and should able to cumulate the transactions up to 7 days.		
142	Proposed Solution should be able to do full binary fingerprint of files and also should be able to detect even if partial information gets leaks from fingerprinted files or folders		

Sr. No	Technical Requirements (DLP)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
143	Proposed solution should be able to enforce policies to detect data leaks even through textual image files through OCR technology.		
144	Proposed Solution should be able to fingerprint only specific fields or columns within a database and should be able to identify information from databases by correlating information residing in different columns in a database.		
145	Proposed solution should enforce policies to detect low and slow volume data leaks over the period for max 7 days.		
146	The solution should have ability to detect cumulative malware information leaks. The solution should able to detect the data leaks over to competitors and the data sent and uploaded after the office hours predefined patterns.		
147	Proposed Solution should have advanced Machine Learning – Ability to automatically learn sensitive information from copies of information that needs to be protected and automatically learn false positives. The solution should enforce policies to detect low and slow data leaks		
148	Proposed solution should have printer agents for print servers to detect data leaks over print channel.		
149	Proposed solution should inspect data leaks over HTTP , HTTPs and SMTP User client like Outlook and Lotus Notes. The solution should be able to inspect HTTP traffic and HTTPs traffic natively . Should provide support both build-in SSL decryption and destination awareness capability with integration with Network and Gateway DLP controls.		
150	Proposed solution should provide capabilities to identify data based on keywords or dictionaries and the solution should be able to enforce policies based on file types, size of files and also the name of the file.		
151	The solution should be able to block outbound emails sent via SMTP if its violates the policy		
152	The proposed solution work as a MTA to receive mails from mail server and inspect content before delivering mails to next hop and should quarantine emails that are in violation of company policy.		
153	The solution should support Email DLP deployment in Cloud Based Mail Messaging Platforms. All licenses required for the same should be included and management should be from the same centralized management platform		

Sr. No	Technical Requirements (DLP)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
154	The solution should be able to identify data leaked in the form unknown and kwon encrypted format like password protected word document.The solution should be able to identify malicious traffic pattern generated by Malware infected PC in order to prevent future data leakage by the malware.The solution should support quarantine as an action for email policy violations and should allow the sender's manager to review the mail and provide permissions for him to release the mail without logging into the UI		
155	The DLP Solution must natively integrate with Cloud based storage solutions like One Drive, Rediff Cloud as well as Box to monitor uploads as well as sharing of data from different assets connected outside the organization. This must be outside endpoint DLP solution.		
156	The solution should be able to enforce policies to detect and prevent data leaks even through image files through OCR technology.		
157	Proposed Solution should support detection of PKCS #12 files (.p12, .pfx) that are commonly used to bundle a private key with its X.509 certificate.		
	AUTOMATED RESPONSE & INCIDENT MANAGEMENT		
158	The incident should include a clear indication of how the transmission or file violated policy (not just which policy was violated), including clear identification of which content triggered the match and should allow opening of original attachment directly from the UI		
159	The incident should display the complete identity of the sender (Full name, Business unit, reporting authority etc.) and destination of transmission for all network and endpoint channels. The solution should also allow assigning of incidents to a specific incident manager		
160	Proposed solution should provide automatic notification to incident managers when a new incident is assigned to them and the incident should not allowed for deletion even by the product administrator		
161	Proposed solution should allow a specific incident manager to manage incidents of specific policy violation, specific user groups etc. The solution should have options for managing and remediating Incidents through email by providing incident management options within the in the notification email itself.		

Sr. No	Technical Requirements (DLP)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
162	Proposed Solution should control incident access based on role and policy violated. The system should also allow a role creation for not having rights to view the identity of the user and the forensics of the incident.The system should create separate roles for technical administration of servers, user administration, policy creation and editing, incident remediation, and incident viewing for data at rest, in motion, or at the endpoint		
163	Incident management should the workflow of the selected incident, then select one of the following options Assign,Change Status,Change Severity,Ignore Incident,Tag Incident,Add Comments,Delete,Download Incident,Lock,unlock		
164	A single event should trigger only one incident, even if it trigger multiple policy and violation. For example, an outbound email could trigger 5-6 policies, e.g. PCI-DSS, PII, etc, but only one single incident will be created. Solution should support CCN# display in violation trigger to be masked in order to stay compliance with PCI-DSS requirement.		
165	The proposed solution should provide Incident Workflow capabilities where user/Business Manager can remediate the DLP policy violations actions from handsets/emails without logging into the Management Console		
166	Proposed solution should provide the ability to detect Policy violation, which retains the source IP address, destination IP address, protocol, sender e-mail address, recipients e-mail address and SMTP Headers.		
167	Proposed solution should provide ability by which Incidents can be assigned automatically to reviewers.		
168	Proposed solution should provide the ability for Incidents to be sorted by severity level, sender, recipient, source, destination, protocol, and content type.		
169	Incident views can be customized based on content pertinent to the reviewer's role and preferences.		
170	Proposed solution should provide an inbuilt Case Management Tool.		
171	Proposed solution should allow a role only to view incidents but not manage or remediate them		
172	Proposed system should allow incident managers and administrators to use their Active directory credentials to login into the console		

Sr. No	Technical Requirements (DLP)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
173	The Proposed DLP engine must performs a post-processing incident grouping step to avoid displaying related incidents in different cases. All incidents from the same user that have the same classification are combined into a group and DLP case card.		
174	Proposed solution should have an option to Encrypt/Quarantine/Monitor/Delete sensitive files found during endpoint discovery.		
175	Solution must have the capability for bulk closure of incidents.		
	REPORTS		
176	Proposed solution should provide detailed reporting options		
177	Proposed system should have options to create a role to see summary reports, trend reports and high-level metrics without the ability to see individual incidents		
178	Proposed system should allow reports to be mailed directly from the UI and should allow automatic schedule of reports to identified recipients		
179	The reports should be exported to at least CSV, PDF, HTML formats		
180	The system should provide options to save specific reports as favorites for reuse		
181	The system should have lots of pre-defined reports which administrators can leverage		
182	The solution should generate reports in PDF, Excel or CSV format.		
183	The solution should develop reports built around stakeholder requirements such as top (X) Policy Violations, Senders, Content Type, Protocol, Historical Reports etc.		
184	Solution should offer flexible audit and reporting capabilities suitable for PCI DSS, SOX, ISO and HIPAA		
185	Allows console users to create and save graphical reports (e.g. pie, bar, line charts)		
186	Allows console users to create and save reports from a list of built-in default reporting templates.		
187	Allow console users to customize and save the reports without the use of third party reporting tools.		
188	Able to generate report on custom retrieved properties that are created by the console user.		

Sr. No	Technical Requirements (DLP)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
189	Allow console users to create filters to include or exclude certain categories of information from the reports.		
190	Allow console users to drill-down from the report to the specific endpoint.		
191	Information reported shall not be more than 1 day old.		
192	Access to reporting function shall be controlled based on rights assigned by the Master Administrator.		
193	The solution shall include a web-based reporting Module		
194	The solution deployment should comply to the ISMS framework		
195	The DLP solution should support as an API be able to provide the risk adaptive based protection by dynamically calling the action plan based on the Risk.		
196	Workflow operations in DLP networking and mobile reports can now be applied to all filtered incidents or to selected incidents only. This includes operations such as: -Assigning incidents -Changing incident status -Changing incident severity -Ignoring incidents -Tagging incidents -Adding comments		
197	Solution should supports components on TLS 1.2 and above		

1.2 Technical and Functional Requirements for Data Identification & Classification Tool (DICT):

Sr. No.	Technical Requirements (DICT)	Bidder's Compliance (Yes/No)	Bidder Remarks if Any
1	The solution should evaluate content, context, identity and other attributes of unstructured data to make classification and policy decisions.		
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.		

Sr. No.	Technical Requirements (DICT)	Bidder's Compliance (Yes/No)	Bidder Remarks if Any
3	The solution should support functionality to check recipients marked in an email and alert/prevent the user from sending the mail if external recipients are marked. Example : An email containing internally classified document as attachment should be prevented from being sent if external recipients are marked in that mail. The user should also get an alert for the same.		
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.		
	DATA CLASSIFICATION AND IDENTIFICATION REQUIREMENTS		
5	The solution should support automated, suggested, and user-driven classification.		
6	The solution should enable the classification of Word, Excel and PowerPoint documents from within Microsoft Office.		
7	The solution should enable the classification of any custom file type.		
8	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.		
9	The solution should support unlimited number of classification fields.		
10	The solution should support users to enforce data retention and disposition tags, including date fields while classifying information especially sensitive information which can result in increased liability if stored longer		
11	The solution should support hierarchical and conditional classification fields, so that the appearance of a sub-field is conditional on the value selected in the higher-level field. For example, when a user selects “Restricted,” a sub-field is presented with a list of departments including “HR Only.”		
12	The solution should support dynamic/tailored classification selections based on the user's Active Directory attributes or groups.		
13	The solution should enable users to assign classification values via a one click classification user interface.		

Sr. No.	Technical Requirements (DICT)	Bidder's Compliance (Yes/No)	Bidder Remarks if Any
14	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.		
15	The solution should enable users to assign classification values to non-classified email in their inbox.		
16	The solution should enable users to set their most frequently used classifications as “Favorites.”		
17	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).		
18	The solution should support 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).		
19	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.		
20	The solution should support the ability to ask users to confirm an automated classification value (also called “suggested classification”).		
21	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.		
22	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.		
23	The solution should support the ability to scan for certain keywords and regular expressions and set the classification accordingly.		

Sr. No.	Technical Requirements (DICT)	Bidder's Compliance (Yes/No)	Bidder Remarks if Any
24	The solution should support creating custom conditions within a policy. For example, the solution should allow creating a custom condition to ensure a particular software is installed on the system before allowing email to be sent, query time of day to ensure an activity takes place during regular business hours.		
25	The solution should generate metadata for all file types, including persistent, embedded metadata for many non-Office files, including PDF, TXT, Visio, Project, images, and multimedia files.		
26	The solution should support the creation of custom metadata for interoperability, including custom X-headers.		
27	The solution should support customizable visual markings in email and documents (e.g. font, size, color, and content).		
28	The solution should support automatic classification of files when its downloaded and saved to specific folders(e.g. Downloads, My Documents) and the classification should be based on file content for files that can be read by a text processor and based on file type or file size or file name or file path for other file types		
29	The solution should support Machine Learning Categorization to help predict different categories of documents, providing classification suggestion or automation on unknown content in documents and email		
30	The solution should have the ability to classify email message with the same classification label as files attached to it		
31	The solution should have the ability to automatically classify email and calendar events as 'Internal' based on the sender and recipient in the same email domain		
32	The solution should have the ability to enforce obtaining consent from end users while handling sensitive information and capture the same in the meta data		
33	The solution should provide the ability to allow user to manually classify file attachment(s) directly within MS Outlook when composing an email without the need to open the attachment and without classifying the original source file.		
	DATA DISCOVERY REQUIREMENTS		

Sr. No.	Technical Requirements (DICT)	Bidder's Compliance (Yes/No)	Bidder Remarks if Any
34	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.		
35	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.		
36	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.		
37	The solution should have the ability to scan Windows file shares, Sharepoint, Sharepoint Online, OneDrive, Dropbox, Box and enforce classification based on content, file attributes, file location		
38	The solution should support Machine Learning Categorization to help predict different categories of documents at rest, providing classification suggestion or automation on unknown documents at rest		
	INFORMATION PROTECTION REQUIREMENTS		
39	The solution should provide interactive warning messages that include remediation options and URL links for additional help and information.		
40	The solution should consolidate all policy warnings in the same policy dialog.		
41	The solution should enable administrators to control whether users can override policy warnings.		
42	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.		
43	The solution should provide the ability to warn/prevent users from downgrading, upgrading, or changing a classification.		

Sr. No.	Technical Requirements (DICT)	Bidder's Compliance (Yes/No)	Bidder Remarks if Any
44	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.		
45	The solution should provide the ability to warn users when opening sensitive Office documents.		
46	The solution should provide the ability to prevent printing of sensitive email and Office documents to specific printers.		
47	The solution should provide the ability to highlight sensitive information within an email and redact the sensitive content so that users can remediate any policy violations before the email leaves the desktop.		
48	The solution should provide advanced control over email attachments via policies that evaluate content, recipients, sender, classification, filename, file size, and other attributes.		
49	The solution should provide the ability to restrict users from sending non-classified email attachments (i.e. attachments that have no classification).		
50	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).		
51	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.		
52	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.		
	AUDITING AND REPORTING REQUIREMENTS		
53	The solution should log user activity while users are handling email, documents, and files.		

Sr. No.	Technical Requirements (DICT)	Bidder's Compliance (Yes/No)	Bidder Remarks if Any
54	The solution should provide flexibility to send user logs to SIEM, syslog server, text file, and Windows event logs as per the need.		
55	The solution should provide a built-in dashboard for reviewing data discovery scanning results for user activity, deployment, data storage trends, and data inventory.		
	CONFIGURATION AND DEPLOYMENT REQUIREMENTS		
56	The solution should provide a centralized, web-based Administration Console for classification configuration and policy management.		
57	The solution should support the ability to save configurations in a single configuration file.		
58	The solution should have the ability to integrate with AD natively and enforce policies based on AD groups and enable administrators to tailor configurations to individual users or groups of users		
59	The solution should cache configurations on endpoints locally for offline use.		
60	The solution should provide the ability to deploy in silent mode either natively or using third party software distribution tools so that software can be deployed and enabled in different phases.		
61	The Solution Should Work with below operating systems: i. Windows 7 / Windows 8 / Windows 8.1 / Windows 10 (All versions) and latest Endpoint OS released by Microsoft time to time. ii. Windows 2008 / 2012/ 2016 / 2019 (All Versions) and latest server OS released by Microsoft time to time. iii. Macintosh OSX.		
62	The Solution Should work with Cloud based mail messaging solutions		
63	The solution should work on Windows 7, 8.1, and 10 Operating Systems		
	INTEGRATION AND INTEROPERABILITY REQUIREMENTS		
64	The solution should provide the ability to attach metadata to information objects, which can be leveraged by the Bidder Proposed third-party data loss prevention (DLP) solutions and should work even when emails and documents are protected.		

Sr. No.	Technical Requirements (DICT)	Bidder's Compliance (Yes/No)	Bidder Remarks if Any
65	Solution should support enforcing policies like encrypt all documents which has PCI information by integrating with IRM solutions		
66	The solution should have the ability to integrate with archival solutions and take actions on archival based on classification label		

1.3 Technical and Functional Requirements for Database Monitoring Solution (DAM):

Sr. No	Technical Requirements (DAM)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
1	The solution should be Database agnostic and should support atleast the following databases:		
1.1	Oracle 8i, 9i, 10g, 11g,12c		
1.2	SQL Server 2000, 2005, 2008 and higher versions		
1.3	Sybase		
1.3	MySQL		
1.5	IBM DB2		
1.6	PostgreSQL		
1.7	Other (specify)		
2	The solution should support on the following OS platforms atleast:		
2.1	IBM AIX		
2.2	Windows NT / 2000, 2003, 2008		
2.3	Red Hat Enterprise Linux		
2.4	SUSE Linux Enterprise		
2.5	HPUX		
2.6	Solaris - SPARC		
2.6	Ubuntu		
3	The solution should be able to provide database security deployed on virtual machines (VMs)		
4	Solution does not require changes in the database application (e.g. truning audit or trace on)		
5	Solution should protect it self from tampering and attacks		
6	Solution allows easy tranlation of actual database acivity into monitoring / audit policy direct from alerts		
7	Solution should be capable of capturing the alerts which will include the following metadata:		

7.1	Originating IP Address		
7.2	DB User		
7.3	OS User		
7.4	Full SQL Statement		
7.5	Accessed tables		
7.6	Application Name		
7.7	Module Name		
7.8	Host Name/Terminal name		
7.9	Command Type		
8	The solution should be capable of sending alerts can be sent to external applications atleast through:		
8.1	via e-mail		
8.2	via syslog		
8.3	via snmp traps		
8.4	Other (specify)		
9	Solution should be capable of monitoring of all database activities and protect against insiders with privileged access		
10	Solution should offer granular monitoring of database transactions with real-time alerts and prevention of breaches		
11	Solution should offer granular monitoring of queries, objects and stored procedures with real-time alerts and prevention of breaches		
12	Solution should provide protection against newly discovered database vulnerabilities, providing immediate protection with no DBMS downtime and without having to update the patch itself.		
14	Solution should provide multiple user roles that facilitate separation of duties		
15	Solution should capable of monitoring and alerting unauthorised access to sensitive data on the Database, like credit card tables etc.m		
16	Solution should have the ability to independently monitor and audit all database activity , including administrator's activity and select transactions.		
17	Solution should record all SQL transactions : DML, DDL , DCL and Selects and The ability to store this activity securely outside the database		
18	Solution should have the ability to enforce separation of duties on Database Administrators. Auditing should include monitoring of DBA activity and solutions should prevent DBA manipulation or tampering with logs or recorded activity.		
	Solution should have the ability to generate alert		

19	on policy violations and provide real time monitoring and rule based alerting.		
20	Solution should have the ability to ensure that a service account only accesses a database from a defined source IP and only runs a narrow group of authorized queries		
21	Solution Should capture and report on SELECT statements made on Databases		
22	Solution Should report on detailed SQL, including the source of the request, the actual SQL commands, the database user name, when the request was sent and what database objects the command was issued against.		
23	Solution Should report on database access including logins, client IP, server IP and source program information.		
24	Solution Should track execution of stored procedures, including who executed a procedure, name of the procedure and when, which tables were accessed as a result		
25	Solution Should track and audit administrative commands such as GRANT,		
26	Solution Should track and report all failed logins.		
27	Solution Should support creation of specific rules on observed events, sending SMTP alerts when the rules are violated.		
28	Solution should Capture and report on non-administrators executing DDL.		
29	Solution Should support architecture where application has pooled connections, the original IP address and user name should be monitored.		
30	The solution deployed should not require any change in the DBMS binaries		
31	The agent should not demand for restart of the database while installing or While upgrading or While uninstalling the solution		
32	Solution should be able to monitor inter and intra DB activities and attacks		
33	Solution should be able to monitor activities done by administrator or any DB admin sitting directly on the database server console		
34	Solution Should be able to scan databases for Vulnerability		
35	Solution should be capable of detecting weak passwords		

36	Ability to protect from all the proposed databases threat vectors to meet RBI compliance requirements. Shall be able to capture all proposed database activities, including from across the network, from local users logged into the server itself, and even from inside the database itself via stored procedures or triggers		
37	Ability to monitor database activities from users using encrypted connections (example Oracle ASO,SSL,SSH etc.		
38	Deliver high performance without inducing any latency, and I/O overheads also shall not require any kernel changes.		
39	Shall have ability to alert via inbuilt dashboard or any other tools. The solution shall also be able to prevent intrusion by terminating sessions and quarantine users that violate security policy.		
40	Shall have ability to protect proposed databases based on older DBMS versions that are no longer supported		
41	The solution shall generate detailed reports, support custom generated reports, expert recommendations for remediation and also reduce time and effort preparing for and responding to compliance audits for the bank		
42	Solution shall have database vulnerability assessment tests for assessing the vulnerabilities and mis-configurations of database servers, and their OS platforms. OS and RDBMS are required to be tested for known exploits and mis-configurations. The product shall identify missing patches.		
43	The solution shall be able to integrate with authentication systems like Active Directory /LDAP		
44	Solution shall be able to integrate with the SIEM solution, Dashboard and Incident Management solution implemented at Bank.		
45	The data transferred between the agent and the appliance shall be through an encrypted channel.		
46	The bidder shall size supply and maintain the required hardware.		

1.4 Minimum Technical requirements for Endpoint Encryption (EE) Solution:

Sr. No.	Technical Requirements (EE)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
1	The solution should be FIPS 140-2 compliant, or FIPS certified		
2	FIPS 140-2 compliant AES 256 algorithm		
3	Solution must have centralized control and can be integrated with authentication engine like AD,LDAP for authentication		
4	Solution should support for different PKI mechanisms.		
4.1	Solution should support for Forced User Lockout through Console		
4.2	Solution should be able to limit number of logon attempts and invoke lockout for failed logon attempts after exceeding the limit (for administrators)		
4.3	Solution should encrypt the entire hard drive		
4.4	Solution should support encryption of extended partitions		
4.5	Solution should prevent access to cached passwords, SAM file, temporary files, and other OS Files at Boot up		
4.6	Solution should provide encryption and access control for other storage media such as USB memory keys, removable external hard drives etc		
4.7	All data should be encrypted in real time		
4.8	Solution should provide single sign on capability		
4.9	Solution should provide password synchronization with domains to simplify having accounts on multiple machines		
5	The solution should be IPv6 compliant		
6	Solution should allow for the recovery of password for a remote user who has forgotten it.		
7	The solution should not provide any facilities to aid in machine recovery in case of stolen machine.		
8	The solution should be able to set the maximum number of administrators, or concurrent administrators		
9	All activities of administrator should be logged.		
10	Solution should log encryption activity and state. Logs should be stored centrally and on endpoint.		
11	Should support all the latest supported versions of the desktop windows operating system		
12	Solution should support encryption of hard disks irrespective of Desktop/Portable Device's OEM/Make/Model.		

Sr. No.	Technical Requirements (EE)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
13	Solution must have the capability to decrypt hard disks at minimum possible period of time in case if Bank requires.		
	Reporting Requirements		
1	Solution should;		
i.	include predefined reports		
ii.	allows for customizing and Ad-hoc reports		
2	The solution shall include a web-based reporting module.		
3	Information reported shall not be more than 1 day old.		
4	Access to reporting function shall be controlled based on rights assigned by the Master Administrator.		
5	The reporting module shall report Total number of endpoints managed and the distribution of these agents;		
6	Allows console users to create and save graphical reports (e.g. pie, bar, line charts)		
7	Allows console users to create and save reports from a list of built-in default reporting templates.		
8	Allow console users to customize and save the reports without the use of third party reporting tools.		
9	Able to generate report on custom retrieved properties that are created by the console user.		
10	Allow console users to create filters to include or exclude certain categories of information from the reports.		
11	Allow console users to drill-down from the report to the specific endpoint.		
12	Allow console users to schedule report generation.		
13	Allow console user to trigger alerts when user-defined conditions are met.		
14	Allow console users to drill-down from the report to the specific endpoint.		
15	Allow console users to schedule report generation.		
16	Allow console user to trigger alerts when user-defined conditions are met.		
	Support Requirements		

Sr. No.	Technical Requirements (EE)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
1	The bidder should have back to back support arrangement with the OEM and provide highest premium support offering 24 * 7 for the solution during the contract period.		
	Compliance Requirements		
1	The Solution should be IPv6 compliant		
2	The proposed solution should integrate with the Bank's Security Information & Event management (SIEM)		
3	The solution deployment should comply to the ISMS framework.		

1.5 Minimum Technical requirements for Patch Management Solution (PMS):

Sr. No.	Technical Requirements (PMS)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
	General Requirements		
1	Solution must provide near real-time (within minutes)visibility, assessment and remediation.		
2	The solution shall operate without requiring agents to belong to a Domain or Active Directory. The solution shall be capable of integrating with one or more Active Directory structures if present; but does not require the schema to be extended. The solution shall operate in with and without domain endpoints.		
3	The solution must include agents that are deployed on all systems to provide OS coverage listed in the scope.		
4	The solution shall support corporate, dial-up, VPN and internet connected users. There should not be the need to purchase additional software/hardware to support users not connected to the corporate network.		
5	The integrity of all policies actuated on the managed computers must be protected by digital signatures at every stage all the way through the distribution points down to the agent. This is necessary to ensure the integrity of the content & packages served to the clients.		

Sr. No .	Technical Requirements (PMS)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
6	The integrity of all packages distributed must be protected using checksums to ensure that the content downloaded has not been modified or corrupted and file sizes are compared to make sure file is downloaded intact.		
7	PKI security mechanisms must be built into the solution, not requiring the purchase of third-party digital certificates.		
8	The solution must have published database schema as well as fully documented API's for integration into other Bank of Maharashtra solutions. This integration may at the agent, database and reporting levels so all need documented and fully open API's.		
	Architecture Requirements		
1	The solution must support a distributed environment, including central and numerous remote sites connected by various network speeds, that may reach/exceed 50000 agents with a single central server and database.		
2	The solution must provide management support in the form of a management station at remote sites without the need for dedicated servers (ie – existing systems) to provide this support; also the solution must support utilizing workstations and laptops at remote sites that have no servers located there.		
3	Ability to throttle bandwidth either statically or dynamically and this throttling must support up and downstream throttling for both the server and agents.		
4	Solution must support the ability cache policies & packages on the management station as needed by the agents or pre-cache content prior to any actions taking place.		
5	The solution must use a single configurable port for agent/server communications.		
6	The agent initiates communications to the server (ie – pull methodology) during normal operational modes; but the solution must support the ability for the server to Push to the		

Sr. No .	Technical Requirements (PMS)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
	agents any new content is available at which point the agents will initiate communications.		
7	The agent must be able to continuously assess and remediate while on or off the network.		
8	The resource utilization used by the agent on the system must be configurable and the agent footprint will be such that memory requirements will be under 20MB and CPU utilization will average to no more than 2%.		
9	The agent can be configured for quiet periods in which no work is done.		
10	The solution must support the following OS:		
a.	Microsoft Windows		
i.	Windows 7 / Windows 8 / Windows 8.1 / Windows 10 (All versions) and latest Endpoint OS released by Microsoft time to time		
ii	Windows 2008 / 2012/ 2016 / 2019 (All Versions) and latest server OS released by Microsoft time to time.		
b.	Macintosh OSX		
c.	UNIX		
i.	Solaris		
ii.	HP-UX		
iii.	IBM AIX		
d.	Linux		
i.	Red Hat (Desktop, Enterprise)		
ii.	Fedora		
iii.	SUSE		
iv.	CentOS		
v.	Ubuntu		
e.	VMWare		
i.	ESXI Server		
12	The solution must support security Patches and Updates for standard Databases including (but not limited to):		
a.	Microsoft SQL server (2000, 2005, 2008, 2012, 2016 and latest SQL versions released by Microsoft time to time)		
b.	Oracle 11g, 12c		
c.	MySql		
d.	DB2		
13	The solution must out-of-the-box support security Patches and Updates for standard desktop applications including (but not limited to):		
a.	Adobe® Reader		

Sr. No .	Technical Requirements (PMS)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
b.	Mozilla Firefox		
c.	Apple iTunes, Quicktime etc.		
d.	Oracle Java™		
e.	Skype		
f.	Real Networks		
g.	WinZip, 7 ZIP, Winrar		
h.	Winamp		
i.	Google Chrome		
j	MS Office		
14	The solution should support patch management on the systems deployed in virtualized environments (VMs)		
15	The solution should support for deploying the customized package (exe or MSI) in all endpoints as per the bank requirement.		
16	Support for including the agent as part of a 'gold' OS image with documented procedures.		
17	Solution should provide an out-of-box agent deployment tool for installing agents . It should be able leverage OU structures from Active Directory, Domain computer groups and manually entered IPs.		
18	The solution should also support the following agent deployment methods – Active Directory Group Policies, login scripts, email, software distribution tools, manually installing the agent.		
19	Single UI for management of all solutions and agents		
20	The solution must have built-in support for higher level of encrypted communications without requiring additional software/hardware.		
21	The solution must support some form of failover capability preferably built-in to the solution.		
22	The solution must provide easy to use upgrade procedures for all components.		
	Administration Requirements		
	Management of Agents		
1	Able to manage all agents from a central console. The central console users shall be able to perform the following tasks (including		

Sr. No.	Technical Requirements (PMS)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
	but not limited to)		
i.	Uninstall agents;		
ii.	Configure all agent settings;		
iii.	Assign agents to Distribution Points;		
iv.	Upgrade agents		
2	Able to monitor the status of all agents from a central console. The console users shall be able to monitor the following information (including but not limited to):		
i.	Last report time of each agent;		
ii.	Availability of each agent;		
iii.	Distribution Point assigned to each agents;		
iv.	Version of each agent.		
v.	Last patch compliance status (Latest applied patches) of the managed assets or endpoints (Desktops, Laptops, Servers).		
3	Administrators have the ability to customize console to fit their individual requirements by adding, removing column headers		
4	Allow console users to initiate ad-hoc (on-the-fly) custom inventory collections for the agents.		
5	Ability for console users to group agents statically by selecting agents and adding to the Manual group or group agents dynamically based upon any number of inventory properties such as (but not limited to) Active Directory groups, OS type, subnet, location, CPU, Applications.		
6	Agents able to dynamically connect to the next nearest Distribution Point if the Distribution Point assigned to the agent is not available.		
7	Able to hide the agent from the agents' "Add/Remove Program" list from the central console.		
8	Security event & inventory information collection from the agents shall be done without inventory or Patch Scans and shall be accurate to the last hour for active client computers.		
9	Allow console users to specify the frequency which the agents communicate with the server.		
10	If the agent fails to communicate to the server within a specified interval, the central		

Sr. No .	Technical Requirements (PMS)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
	console shall automatically mark the agents as offline and this specified interval is configurable by the console user.		
11	End-users shall NOT have an interface to the agents' settings. However, notifications to end-user should be shown on need basis.		
12	Administrator is able to manually assign the agents to a management station based on any computer property e.g Subnet address, OS, Applications/Application version etc.		
13	Ability to provide end-user interface that allows the user to accept or pull actions pre-approved by the console admins. e.g. On-demand Software distribution by end-user.		
	Management of Distribution Points		
1	Able to manage all Distribution Points from a central console. The console users shall be able to perform the following tasks from the central console (list not exhaustive):		
i.	Setting up of Distribution Points;		
ii.	Decommissioning Distribution Points;		
iii.	Configuring settings on any Distribution Points;		
iv.	Upgrading Distribution Points.		
2	Able to monitor the status of Distribution Points from a central console. The console users shall be able to monitor the following information (list not exhaustive):		
i.	Hard disk space available on the Distribution Points;		
ii.	Number of agents attached to each Distribution Point;		
iii.	Availability of each Distribution Point.		
iv.	Version of agent software installed on the Distribution Points.		
3	The Distribution Points should be able to run on any existing shared Microsoft Windows but not limited to OS Windows 7, Windows 8, Windows 10, or Windows 2008/2012/2016 Server.		
4	The Distribution Point should be able to run on other shared computers running non windows platforms like RHEL, SOLARIS,		

Sr. No.	Technical Requirements (PMS)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
	AIX, SUSE, Apple Mac OSX etc.		
5	Ability to On-the-fly move the Distribution Point content cache folder to a different drive having highest space if current drive is out of space.		
	Management Console		
1	RBAC (Role Based Access Control) is supported thus providing different levels of users including the creation of 'read only' users.		
2	The solution should allow use of LDAP / Active Directory or internally created users to authenticate and authorize console users.		
3	RBAC should ensure that the authority to customize policies is restricted to the authorized users only.		
4	The console user shall be able to delegate administrative roles to users to administer only either individual agents or specific groups of agents.		
6	Able to view the activities of each console user and console operator and export the information.		
7	The solution must support the ability to apply large number of individual policies as a group with the intent of creating a policy baseline / standard for the computers.		
8	The solution must support the ability to create custom folders / containers that can be used to store any/all policies that have been approved.		
9	Role based Access Control should ensure that only designated users will perform authorized actions on computers assigned to them		
	General Reporting Requirements		
1	The solution shall include a web-based reporting module.		
2	Information reported shall not be more than 1 day old.		
3	Access to reporting function shall be controlled based on rights assigned by the Master Administrator.		

Sr. No .	Technical Requirements (PMS)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
4	The reporting module shall contain, but not limited to, the following reports:		
5	Progress of all patches applied;		
i.	Number of vulnerabilities detected by month;		
ii.	Total number of agents managed and the distribution of these agents;		
iii.	Top 10 most common vulnerabilities detected;		
iv.	List of software installed on each agent.		
6	Allows console users to create and save graphical reports (e.g. pie, bar, line charts)		
7	Allows console users to create and save reports from a list of built-in default reporting templates.		
8	Allow console users to customize and save the reports without the use of third party reporting tools.		
9	Able to generate report on Hardware and Software inventory information.		
10	Allow console users to generate customized reports on Hardware and Software inventory information.		
11	Able to generate report on custom retrieved properties that are created by the console user.		
12	Allow console users to create filters to include or exclude certain categories of information from the reports.		
13	Allow console users to drill-down from the report to the specific agents.		
14	Allow console users to schedule report generation.		
15	Allow console user to trigger alerts when user-defined conditions are met.		
16	Able to render the status of selected agents based on a selected retrieved property or vulnerability status. (e.g. disk space available, unpatched machines etc in different colors)		
17	Able to display the agents according to hierarchy based on a selected retrieved property such as AD path, IP subnet, or other retrieved property.		
	Patch Management Requirements		
	Patch Detection		
1	Solution should provide out-of-box patch assessment without the need to setup/schedule and maintain scan process,		

Sr. No .	Technical Requirements (PMS)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
	this assessment should report back near real-time (within minutes) once the agent has downloaded its policies.		
2	The solution shall use all of the following methods to determine if a patch has been installed on a agent:		
a.	Inspecting the registry.		
b.	Examining if the required files exist.		
c.	Inspecting the version number of existing files on the agent.		
3	Able to determine patch dependencies prior to deployment of patches to the agents.		
4	Able to determine if a patch has already been installed on an agent		
5	Able to determine if a newer patch has been installed on an agent and if so, the solution shall treat the agent as patched.		
6	Able to determine if the patches on the agents are correctly installed.		
7	Able to detect the required patches according to individual agent’s configuration.		
8	Solution must detect if a patch that has been applied becomes corrupt.		
9	Solution must able to detect and report if a patch uninstalled from system. Solution should able to provide report of information uninstalled patches of managed asset (Desktop, Laptop, Servers) in addition to alert.		
	Patch Deployment		
1	Solution must be able to manually group agents together for deployment of patches.		
2	Solution must provide the ability to dynamically group agents based on asset and software information.		
3	Groups shall be automatically updated once the members’ asset or software information is changed.		
4	The solution must support grouping of patches into a single group for e.g - all patches Critical severity patches released in Jan XXXX can be grouped together and deployed in one action.		

Sr. No.	Technical Requirements (PMS)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
5	Descriptions and severity levels of the patches shall be available within the solution. A hyperlink to the patch information on software vendors' websites shall be provided.		
6	The solution must support the ability to make changes to the properties of patch policies to reflect Bank of Maharashtra's own patch definitions.		
7	Solution must support the ability align testing & deployment flow procedure that will reflect Bank of Maharashtra approval process.		
8	All patches shall be thoroughly tested before the patch information is made available and Console users shall be informed of any problems encountered during testing by way of highlighted Notices.		
9	Allow console user to deploy patches to all agents via a central console.		
10	Allow console user to deploy patches without intervention from the users.		
11	Allow console user to target which agents to deploy the patches to.		
12	Allow console user to set a validity window for each action deployed in order to maintain control over actions and automatically expire actions that have passed outside the validity window.		
13	Allow console user to define different patch deployment policies for different computers in the same location.		
14	Able to provide real-time (within minutes) patch deployment status monitoring		
15	Able to identify real-time (within minutes) the agents which have completed the installation of patches, but are pending restart. Once the system has been restarted the agent will immediately re-run the patch policy to make sure all necessary actions were successful at which point it will report back successful.		
16	Allow console users to deploy multiple patches at one time without the need to restart the agents.		
	Allow console users to spread the patch		

Sr. No.	Technical Requirements (PMS)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
17	deployment over a pre-defined period of time to reduce overall impact to network bandwidth.		
18	Allow console users to customize the message displayed in a pop-up message box to all users before the installation of any patch.		
19	Allow users to postpone the deployment of a patch for a period of time determined by the console user.		
20	Allow console users to restart the selected agents from the central console.		
21	Allow console users to shut down the selected agents from the central console.		
22	Allow users to postpone the restarting of their agents for a period of time determined by the console user		
23	Able to re-deploy the patch on a agent automatically if the initial deployment is not successful.		
24	Able to re-deploy the patch on a agent automatically even if the deployed patch is uninstalled by the user.		
25	Allow console user to create a custom actions to deploy their own patches.		
26	Able to cache the patches in the various Distribution Points.		
27	Able to install all previously deployed patches automatically to agents that are subsequently added to the network.		
28	Able to delete the patch installation files from the agents' hard disk automatically once the patch has been successfully applied.		
29	Administrator must be able to target the particular patch on all the machines with any specific properties.		
30	The system must be intelligent to check the relevance of the computer before deploying a patch after download on the endpoint.		
	Patch Rollback		
1	Able to identify the agents that have installed the patch that is to be rolled back.		
2	Allow console users to monitor the progress of the roll-back action from the central console.		
3	Provide users with wizard to generate patch rollback policy.		

Sr. No .	Technical Requirements (PMS)	Bidder's Compliance (Yes/No)	Bidder Remarks, if any
4	Able to report if the roll-back is successful on the targeted agents.		
	Support Requirements		
1	The bidder should have back to back support arrangement with the OEM and provide highest premium support offering 24 * 7 for the solution during the contract period.		
	Compliance Requirements		
1	The Solution should be IPv6 compliant		
2	The proposed solution should integrate with the Bank's Security Information & Event management (SIEM)		

Annexure 2: Technical Bid Format

Information	Details to be furnished by the bidder
Name of the bidder	
Year of establishment and constitution Certified copy of "Partnership Deed" or "Certificate of Incorporation" should be submitted as the case may be	
Location of Registered office /Corporate office and address	
Mailing address of the bidder	
Names and designations of the persons authorized to make commitments to Bank	
Telephone and fax numbers of contact persons	
E-mail addresses of contact persons	
Description of business and business background Service Profile & client profile Domestic & International presence Alliance and joint ventures	
Gross revenue of the bidder (not of the group) 2016-2017 2017-2018 2018-2019	
Net Profit of the bidder (not of the group) 2016-2017 2017-2018 2018-2019 Documentary proofs are to be enclosed	
Details of the similar assignments executed by the bidder (Name of the Bank, time taken for execution of the assignment and documentary proofs from Bank are to be furnished)	
Details of the bidder's proposed methodology/approach for providing services to Bank with specific reference to the scope of work.	

Declaration:

We confirm that we will abide by all the terms and conditions contained in the RFP.

We hereby unconditionally accept that Bank can at its absolute discretion apply whatever criteria it deems appropriate, not just limiting to those criteria set out in the RFP, in short listing of bidders.

All the details mentioned by us are true and correct and if Bank observes any misrepresentation of facts on any matter at any stage, Bank has the absolute right to reject the proposal and disqualify us from the selection process.

We confirm that this response, for the purpose of short-listing, is valid for a period of 180 days, from the date of expiry of the last date for submission of response to RFP.

Place:

Date: Seal & Signature of the bidder

Annexure 3: Conformity with Hard copy Letter

(Pro-forma of letter to be given by all the Bidders, participating in the RFP for supply, installation, commissioning and maintenance of security solution (DLP, DICT, DAM, EE & PMS), on their official letterheads)

To

General Manager (IT),

Bank of Maharashtra Information Technology,

Head Office,

Lokmangal, Shivaji Nagar, Pune - 411005

Dear Sir,

Sub: RFP NO: XX for supply, installation, commissioning and maintenance of security solution (DLP, DICT, DAM, EE & PMS) dated: XX.

Further to our proposal dated __________, in response to the Tender Document No: XX, dated: XX issued by Bank of Maharashtra (**“Bank”**) we hereby covenant, warrant and confirm as follows:

The soft-copies of the proposal submitted by us in response to the Tender Document No: XX, dated XX and the related addendums and other documents including the changes made to the original tender documents issued by the Bank, conform to and are identical with the hard-copies of aforesaid proposal required to be submitted by us, in all respects.

Yours faithfully,

Authorized

Signatory

Designation

Bidder’s corporate name

Annexure 4: Conformity Letter

(Pro-forma of letter to be given by all the bidders, participating in the RFP for supply, installation, commissioning and maintenance of security solution (DLP, DICT, DAM, EE & PMS), on their official letter-head)

To

General Manager (IT),

Bank of Maharashtra Information Technology, Head Office,

Lokmangal, Shivaji Nagar, Pune - 411005

Dear Sir,

Sub: RFP NO: XX for supply, installation, commissioning and maintenance of security solutions (DLP, DICT, DAM, EE & PMS) dated: XX.

Further to our proposal dated __________, in response to the tender Document No: XX, dated: XX (hereinafter referred to as **"TENDER DOCUMENT"**) issued by Bank of Maharashtra (**"Bank"**) we hereby covenant, warrant and confirm as follows:

We hereby agree to comply with all the terms and conditions / stipulations as contained in the TENDER DOCUMENT and the related addendums and other documents including the changes made to the original tender documents issued by Bank, provided however, that only the list of deviations furnished by us in Annexure 12 of the main TENDER DOCUMENT which are expressly accepted by Bank and communicated to us in writing, shall form a valid and binding part of the aforesaid TENDER DOCUMENT. Bank is not bound by any other extraneous matters or deviations, even if mentioned by us elsewhere either in our proposal or any subsequent deviations sought by us, whether orally or in writing, and the Bank's decision not to accept any such extraneous conditions and deviations will be final and binding on us.

Yours faithfully,

Authorized

Signatory

Designation

Vendor's corporate name

Annexure 5: Eligibility Criteria Compliance

The Bank will examine the Eligibility Criteria compliance for the bidder and OEM as per the below tabulated criteria in this RFP. The Bidder(s) and OEM's who satisfy the eligibility criteria conditions shall be considered for the next phase of evaluation viz. Technical Evaluation.

The Bidder / OEM is required to meet ALL the following eligibility criteria applicable to them and provide adequate documentary evidence for each of the criteria stipulated below:

S No.	Eligibility Criteria	Supporting Documents
A	**Criteria to be met by the Bidder**	
1	Bidder should be registered in India. Bidder must be a Government Organization / PSU/ PSE / partnership firm / LLP/ Limited Company/Pvt Ltd Company	Valid Certification of incorporation as on date of bid submission. Note:in case of mergers/ acquisitions/restructuring or name change & the date of establishment of earlier/original entity can be considered
2	The bidder should have been in existence for a minimum period of five years in India as on 31-Mar-2020	Certificate of incorporation
3	The minimum annual turnover of Bidder should not be less than INR 75 crores in each of the last three financial years, viz., 2016-17, 2017-18 and 2018-19 from India operations	Audited Financial Statements or CA certificate for the financial years 2016-17, 2017-18 and 2018-19.
4	Bidder should have positive net worth for last three financial years i.e. 2016-17, 2017-18 and 2018-19	Audited Financial Statements or CA certificate for the financial years 2016-17, 2017-18 and 2018-19.
5	The Bidder should be an authorized partner with the highest partnership level of OEM for at least the last 3 years from the date of this RFP. This partnership may be Indian or Global.	Letter from OEM stating that the Vendor is an authorized partner with the highest partnership level of OEM, along with the date of the partnership.
6	Bidder should not have been black-listed by any Public Sector Bank, RBI/ NHB, IBA or any regulatory authority as on date of RFP submission.	Self-Declaration on Bidder's letter head signed by the authorized signatory. Bank may verify the information through publicly available data and information.

S No.	Eligibility Criteria	Supporting Documents
7	Neither the Bidder, nor their promoters and Directors should be defaulters to any financial institution. The Bidder should not have been reported against by any Public-Sector Bank to Indian Banks Association for any malpractice, fraud, poor service, etc. An undertaking (on their letter head) in this regard should be enclosed by the bidder on behalf of the directors/partners blacklisted by any Government authority or public sector undertaking (PSU) as on date of submission of tender, otherwise the bid will not be considered. An undertaking (on their letter head) in this regard should be enclosed by the bidder on behalfof directors/partners. The Bidder should not have been blacklisted by any Government authority or Public sector Undertaking (PSU) as on date of submission of the tender, otherwise the bid will not be considered. An undertaking (on their letter head) in this regard should be enclosed by the Bidder on behalf of the directors/partners.	Self-Declaration letter signed by Authorized Signatory to be submitted.
8	The Bidder should not have been declared Non-Performing Asset (NPA) by any BFSI organization as on date of submission of the tender, otherwise the bid will not be considered.	Self-Declaration letter signed by Authorized Signatory to be submitted.
9	Bidder Should have at least one of the following accreditations / certifications which are valid as on the date of issue of this RFP. ISO, SEI CMM, BS 7799.	Copy of certifications

S No.	Eligibility Criteria	Supporting Documents
10	The Bidder should have the experience of implementing at least 3 out of the 5 solutions in at least one at least one Govt. Sector/Scheduled Commercial Bank/PSU's in India. The credentials provided could be in the same or different Govt. Sector/Scheduled Commercial Bank/PSU's in India. 1. DLP 2. DICT 3. DAM 4. EE 5. PMS The solutions deployed may not necessarily have to be the same proposed product.	Relevant Credential letters OR Purchase Order with the Bank's confirmation on having executed the PO to satisfaction
11	The bidder should have a minimum of 10 individuals with prior experience in implementation of proposed security solution. All resources must be on the payroll of the bidder.	Certificate from the Company Auditors / Company Secretary / HR mentioning number of resources having experience in proposed security solution.
12	The proposed bidder should have office in India and should be able to support project in India during the contract period.	An undertaking letter to be enclosed by the Bidder confirming the same.
13	The bidder should have minimum 2 skilled OEM trained/ certified staff for the Security solution proposed under this RFP.	(CV along with training/certificate details Certificate from OEM (who will be on project in Bank Of Maharashtra
B	**Criteria to be met by the OEM**	
1	The proposed DLP application should be live in at least one Govt. Sector/Scheduled Commercial Bank/PSU's in India.	Relevant Credential letters OR Purchase Order with the Bank's confirmation on having executed the PO to satisfaction.
2	The proposed DAM application should be live in at least one Govt. Sector/Scheduled Commercial Bank/PSU's in India.	Relevant Credential letters OR Purchase Order with the Bank's confirmation on having executed the PO to satisfaction.

S No.	Eligibility Criteria	Supporting Documents
3	The proposed DICT solution should be live in at least one BFSI organization in India.	Relevant Credential letters OR Purchase Order with the Bank's confirmation on having executed the PO to satisfaction
4	The proposed for EE solution should be live in at least one Govt. Sector/Scheduled Commercial Bank/PSU's in India.	Relevant Credential letters OR Purchase Order with the Bank's confirmation on having executed the PO to satisfaction
5	The proposed PMS solution should be live in at least one Govt. Sector/Scheduled Commercial Bank/PSU's in India.	Relevant Credential letters OR Purchase Order with the Bank's confirmation on having executed the PO to satisfaction
6	The proposed OEMs should have presence in India and outside India and should be able to support project from India during the contract period. OEM must have own technical support centre in India.	An undertaking letter to be enclosed by the OEM confirming the same.
7	The OEM should have been in existence for a minimum period of five years in India as on 31-Mar-2020.	Certificate of incorporation

Note:

All eligibility requirements mentioned above should be complied by the bidders as applicable and relevant support documents should be submitted for the fulfilment of eligibility criteria failing which the Bids may be summarily rejected. Non-compliance of any of the criteria can entail rejection of the offer. Photocopies of relevant documents / certificates should be submitted as proof in support of the claims made for each of the above-mentioned criteria and as and when the Bank decides, originals / certified copies should be shown for verification purpose. The Bank reserves the right to verify / evaluate the claims made by the Bidder independently. Any deliberate misrepresentation will entail rejection of the offer ab-initio. Other conditions are as below :

1. Documentary evidence must be submitted for each criterion.
2. Banks exclude Cooperative Banks & RRBs. PSB means Public Sector Banks, including RBI.
3. Public/private sector banks mean public/private sector banks in India only.
4. Proposed solution need not be the proposed version of the solution can be any version of the solution.

Annexure 6: Cover Letter

RFP NO: XX Dated: XX

To,
General Manager (IT),
Bank of Maharashtra Information Technology,
Head Office,
Lokmangal,
Shivaji Nagar,
Pune - 411005

Dear Sir,

1. Having examined the Tender Documents including all Annexures, the receipt of which is hereby duly acknowledged, we, the undersigned offer to supply, implement and maintain all the items mentioned in the 'Request for Proposal' and the other schedules of requirements and services for your bank in conformity with the said Tender Documents in accordance with the schedule of Prices indicated in the Price Bid and made part of this Tender.

2. If our Bid is accepted, we undertake to abide by all terms and conditions of this tender and also to comply with the delivery schedule as mentioned in the Tender Document.

3. We agree to abide by this Tender Offer for 180 days from date of Tender (Commercial Bid) opening and our offer shall remain binding on us and may be accepted by the Bank any time before expiry of the offer.

4. This bid, together with your written acceptance thereof and your notification of award, shall constitute a binding contract between us.

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

6. We certify that we have provided all the information requested by the bank in the format requested for. We also understand that the bank has the exclusive right to reject this offer in case the bank is of the opinion that the required information is not provided or is provided in a different format.

Dated this…………………………………..by ……………………….20

Authorized Signatory

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

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

Signature & Seal of Bidder

Annexure 7: Application Management Services

The successful bidder must provide FM services and shall only be allowed to connect to Bank's network from Bank locations only. The bidder shall not be allowed to establish a remote connection from any third party delivery centres in order to provide such services.

The bidder is required to propose on-site delivery model. The following table provides indicative activities under Application Management Services. The scope of work shall be inclusive of, but not limited to, the activities mentioned under the service category.

However, bidder must deploy atleast one Project Manager Resources and atleast one Enterprise Architecture, full-time, during the entire contract duration in order to ensure complete delivery of scope of work pertaining to application management services and to meet the SLA requirement. The bidder is expected to deploy online tool to track service incident and problem resolution and reporting of SLA. The service window for FM services shall be 24x7x365.

Bidder's responsibility should include:

- Provide Application Management services to manage proposed solution
- Provide relevant reports for the previous month in the 1st week of every month and review it with the Bank in next 3 working days
- Benchmark reports against the service levels defined in the RFP and calculate the liquidated damages based on the level of deviation from Service levels defined
- Submit the list of reports to track performance on service levels for all managed services under scope of this RFP

Application Management Services	
1	Performing client installation/re-installation, configuration & un-installation of applications and access management
2	Performing OEM interaction for resolving application and infrastructure related issues
3	Performing performance tuning of applications
4	Processing change request, bug fixing and vulnerability assessment
5	Performing 24*7 performance monitoring and management of application
6	Performing patch updates and software updates for in-scope application
7	Resolving issues related to integration with other business application, report generation, workflows, report creation, report customization and assignment of /modification in roles & responsibilities
8	Resolving incidents and problems related to proposed security solutions
9	Supporting Disaster Recovery activities by DR set-up creation and DR management including DR synchronization, DR drills (performed quarterly), etc.
10	Performing any other day-to-day administration and support activities
11	Configuring and managing HTTP
12	Configuring and using monitoring tools provided for hardware and application management
13	Backup & restoration management of application users

14	Receiving incidents through phone, web, tools or e-mail. Enter the incidents in the online tool and inform Bank of the unique incident id generated through email
15	Assign priority based on agreed upon definitions and route the request to the appropriate service engineer (including for on-site or on call support) and track till resolution
16	Providing updates to Bank on incidents logged
17	Performing performance management
18	Performing version migration, testing and implementation
19	Performing file-level backup for application server
20	Performing portal/content management
21	Performing user management
22	Providing support to known errors and problems
23	Monitoring alert notifications, checking for impending problems, triggering appropriate actions
24	Periodic assessment and review of the solution deployment and mapping with RBI/ regulatory guidelines every six months during the entire tenure of the contract.
25	Data Collection from Business Units, Policy/Rule creation, Policy/Rule Testing, Policy/Rule Fine-Tuning Tasks and Support in closure of alerts/incidents triggered out of the Policies/Rules defined.
26	All other tasks inline with the Scope of work and technical requirements as mentioned in the RFP

Annexure 8: Pre-bid Query Format

Comments on the Terms & Conditions, Services and Facilities provided:

[Please provide your comments on the Terms & conditions for RFP NO: XX dated: XX in this clause. You are requested to categorize your comments under appropriate headings such as those pertaining to the Scope of work, Approach, Work plan, Personnel schedule, Terms & Conditions etc. You are also requested to provide a reference of the page number, state the clarification point and the comment/ suggestion/ deviation that you propose as shown below.]

S. No.	Page #	Point / Clause #	Clarification point as stated in the tender document	Comment/ Suggestion/ Deviation
1				
2				
3				
4				
5				
6				
7				
8				
9				

Dated:

Authorized Signatory

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

Annexure 9: Bid Security Form

(FORMAT OF BANK GUARANTEE (BG) FOR BID SECURITY.)

(ON A NON-JUDICIAL STAMP PAPER OF RS.500.00)

Guarantee for Payment of Earnest Money/Security Deposit

Bank Guarantee no.:

Date:

Period of Bank Guarantee: Valid up to

Amount of Bank Guarantee: Rs. 50,00,000/-

To,
Bank of Maharashtra,
IT Department,
1501, Lokmangal,
Shivajinagar, Pune 411005.

THIS DEED OF GUARANTEE made at …….. this ………..day of ………….. between Bank of ……………………… a banking company having its office at ……………… hereinafter referred to as 'the Bank' of the One Part and Bank of Maharashtra a New Bank constituted under the Banking Companies (Acquisition & Transfer of Undertakings) Act, 1970 having its Head Office at 'Lokmangal', 1501 Shivajinagar, Pune 411 005, hereinafter called the Beneficiary, of the other Part.

1. Whereas the Beneficiary had invited tenders for supply, installation, commissioning and maintenance of various security solutions(DLP, DICT, DAM, EE & PMS), vide tender No: _____ dated: _______
2. One of the terms of the tender is that bidder are required to give a Bank Guarantee drawn in favour of beneficiary and payable at Pune, (valid for 180 days from the due date of the tender) for Rs 50,00,000- (Rs. Fifty Lakhs only) as Earnest Money Deposit (EMD) along with their offer. The Beneficiary may accept Bank Guarantee in lieu of EMD for an equivalent amount issued by any Public Sector Bank, valid for 6 months from the date of issue.
3. M/s <Bidder Name>. hereinafter referred to as the said 'Contractors' have given their offer to supply, installation, commissioning of Servers at given locations to the Beneficiary and the said Contractors are required to deposit the said amount of earnest money (or security deposit) or to furnish bank guarantee.
4. At the request of the said M/s. <Bidder Name>. Ltd. the Bank has agreed to furnish guarantee for payment of the said amount of earnest money (or security deposit) in the manner hereinafter appearing:

NOW THIS DEED WITNESSETH that pursuant to the said tender and in consideration of the premises the Bank doth hereby guarantee to and covenant with the Beneficiary that the Bank shall, whenever called upon by the Beneficiary in writing and without demur and notwithstanding any objection raised by the said Contractor/s, pay to the Beneficiary the said amount of Rs 50,00,000- (Rs. Fifty Lakhs only) payable by the said Contractor/s under the said Contract.

AND IT IS AGREED and declared by the Bank that the liability of the Bank to pay the said amount whenever called upon by the Beneficiary shall be irrevocable and absolute and the Bank will not be entitled to dispute or inquire into whether the Beneficiary has become entitled to forfeit the said amount as earnest money (or as security deposit) under the terms of the said contract or not and entitled to claim the same or not or whether the said contractors have committed any breach of the said contract or not or whether the Beneficiary is entitled to recover any damages from the said contractors for breach of terms thereof or not.

Any such demand made by the Beneficiary shall be binding and conclusive as regards amount due and payable by the Contractor to the Beneficiary. And the Bank undertakes to pay unconditionally on written demand without demur and the claim of beneficiary shall be conclusive and binding as to the amount specified therein.

AND it is further agreed and declared by the Bank that any waiver of any breach of any term of the said contract or any act of forbearance on the part of the Beneficiary or any time given by the Beneficiary to the contractors for carrying out and completing the work under the said contract or any modifications made in the terms and conditions of the said contract or any other act or omission on the part of the Beneficiary which could have in law the effect of discharging a surety, will not discharge the Bank.

AND it is agreed and declared that this guarantee will remain in force until the time fixed in the said contract for completion of the said work or until the expiration of any extended time for such completion and shall be valid for a period of six months from the date hereof i.e. the guarantee shall be valid up to ……

AND it is agreed and declared that this Guarantee will be irrevocable and enforceable even if the contractor’s company goes into liquidation or there is any change in the constitution of the said Company or management of the said Company and shall ensure to the benefit of its successors and assigns and shall be binding on the successors and assigns of the Bank.

Notwithstanding anything contained herein:

a) *The Bank’s liability …………………. not exceed Rs. …………. (Rupees…………………………….)*
b) *This Bank Guarantee shall be valid up to ……………………… and*
c) *The Bank ……………………. on or before ……………. (Date of Expiry of Guarantee)*
d) ***Every Guarantee shall be issued (regardless of the guarantee period) with a minimum claim period of one year from the date of expiry on top of the guarantee period so as to avail benefit of Exception 3of the Section 28 of the Indian Contract Act, 1872. In other words, The Bank issuing such guarantee will not be liable under such guarantee to the beneficiary after the expiry of the claim period of one year, regardless of period of limitation under the Limitation Act, 1963. Commission for the claim period also be charged to the customer.***

   Or

   If a Bank Guarantee is issued with a claim period of less than one year on top of the guarantee period, then such guarantee will not have the benefit of Exception 3 of the Section 28 of the Indian Contract Act, 1872. In other words, The Bank issuing such guarantee could stand exposed to period of limitation under the Limitation Act, 1963, which period is 30 years when

the Government is the guarantee beneficiary and 3 years when any other party is the guarantee beneficiary.”

IN WITNESS WHEREOF the Bank has put is seal the day and year first hereinabove written. Signed, sealed and delivered by Mr…………

For and on behalf of the Guarantor Do so and

to affix the seal of the Bank, in the presence of ……….

Annexure 10: Commercial Bill of Material

(Attached as a separate file with this RFP)

Annexure 11: Compliance Statement for Reverse Auction

(To be submitted by all the bidders participating in Reverse Auction)

To,
General Manager (IT),
Bank of Maharashtra
Information Technology,
Head Office,
Lokmangal, Shivaji
Nagar, Pune – 411005

Sub: RFP NO: XX for supply, installation, commissioning and maintenance of security solutions (DLP, DICT, DAM, EE & PMS), dated: XX

We ______________________ (name of the company) hereby confirm having submitted our bid for participating in Bank's RFP dated _________ for procurement of ____________.

1 We also confirm having read the terms of RFP as well as the Business Rules relating to the Reverse Auction for this RFP process.

2 We hereby undertake and agree to abide by all the terms and conditions stipulated by Bank of Maharashtra in the RFP document including all annexures and the Business Rules for Reverse Auction.

3 We shall participate in the on-line auction conducted by ……………….. (Auctioneer Company) and submit our commercial bid. We shall also abide by the procedures prescribed for online auction by the auctioneer company.

4 We, hereby confirm that we will honour the Bids placed by us during the auction process, failing which Bank shall forfeit the Earnest Money Deposit. We also understand that the bank may debar us from participating in future tenders.

5 We confirm having nominated Mr. ________________, designated as ______________ of our company to participate in the Reverse Auction on behalf of the company. We undertake that the company shall be bound by the bids made by him in Reverse Auction.

6 We accordingly authorize Bank and/ or the reverse auction company to issue user ID and password to the above named official of the company.

7 Both Bank and the auction company shall contact the above named official for any and all matters relating to the Reverse Auction.

8 We, hereby confirm that we will honour the Bids placed by Mr. __________ on behalf of the company in the auction process, failing which Bank will forfeit the EMD. We agree and understand that the bank may debar us from participating in future tenders for any such failure on our part.

9 We undertake to submit the confirmation of last bid price by us to the auction company/Bank within 24 working hours of the completion of event. We also undertake to submit the Bill of Materials for the TCO (Total Cost of Ownership) in terms of RFP.

Name of Authorized Representative: ______________________

Signature of Authorized Representative: ___________________

Verified above signature

Place:

Date:

Seal and signature of the bidder

Annexure 12: List of Deviations Requested

To,
General Manager (IT),
Bank of Maharashtra
Information Technology,
Head Office,
Lokmangal, Shivaji
Nagar, Pune – 411005

Sub: RFP NO: XX supply, installation, commissioning and maintenance of various security solutions(DLP, DICT, DAM, EE & PMS), dated: XX

[Please provide your comments on the Terms & Conditions in this clause. You are requested to categorize your comments under appropriate headings such as those pertaining to the Detailed Scope of work, Service levels, Instruction to Bidders, Curriculum Vitae, Experience in related projects, etc. You are also requested to provide a reference of the page number, state the clarification point and the deviation that you propose as shown below.]

S.No.	Page #	Point / Clause #	Clarification point as stated in the tender document	Deviations requested	Justification
1					
2					
3					
4					
5					
6					
7					
8					

Yours faithfully,

Authorized Signatory

Designation
Bidder’s name

Annexure 13: Pre Contract Integrity Pact

(To be stamped in accordance with the stamp act)

General:

This pre-bid pre-contract Agreement (hereinafter called the Integrity Pact) is made on _____ day of month of _________ 2020, between on one hand, Bank of Maharashtra through authorized official Shri Shri. ______________________________, General Manager, Information Technology Department, Bank of Maharashtra (hereinafter called the "BUYER", which expression shall mean and include unless the context otherwise required, his successors in office and assigns) of the First Part and M/s__________________ represented by Shri. ___________________ Chief Executive Officer (herein 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) 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/LLP, constituted in accordance with the relevant law in the matter and the BUYER is an Information Technology Department of Bank of Maharashtra

NOW, THEREFORE,

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

Enabling the BUYER to obtain the desired said Equipment/product/services 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 hereto herby agree to enter into this Integrity Pact and agree as follows:

Commitments of the BUYER:

1.1. The BUYER undertakes that no officials of the BUYER, connected directly or indirectly with contract will demand, take a promise for or accept directly or through intermediaries any bribe, consideration gift reward favor or any material or immaterial benefit or any other advantage from the Bidders 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 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 official(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 favor, any material or immaterial benefit or other advantage, commission fees, brokerage or inducement to any official of the BUYER, connected directly or indirectly with bidding process, or to any person organization or third party related to the contract in exchange for any advantages 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, favor, any material benefit or other advantage commission fees brokerage or inducement to any officials 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 favor or disfavor to any person in relation to the contract or any other contract with 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 bid/contract.

3.5. The BIDDER further confirms and declares to the BUYER that the BIDDER is the original manufacturer/integrator and 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 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 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 BIDDER's firm, the same shall be disclosed by the BIDDER at the time of filing of tender.

The term 'relative; for this purpose would be as defined in Clause 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 ______ (*to be specified in RFP) as* Earnest Money Deposit/ Security Deposit, with the BUYER through any of the following instruments:

5.1.1. Bank Draft or Pay Order in Favor of **Bank of Maharashtra IT Department** **5.1.2.** 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 demure whatsoever and without seeking any reason whatsoever. The demand for payment by the BUYER shall be treated

as conclusive proof of payment.

5.1.3. Any other mode or through any other instrument (to be specified in the RFP)

5.2. The Earnest Money/Security Deposit shall be valid up to a period of six years or the complete conclusion of the contractual obligations to the complete satisfaction of both the BIDDER and the BUYER, including warranty period, whichever is later.

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 decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

4.2. No interest shall be payable by the BUYER to the BIDDER in 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 its or action on its behalf (Whether with or without the knowledge of the BIDDER) shall entitled the BUYER to take all or any one of the following actions, wherever required :-

6.1.1. To immediately call of 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.

6.1.2. 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 assigning any reason therefore.

6.1.3. To immediately cancel the contract, if already signed, without giving any compensation to the BIDDER.

6.1.4. 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 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 project such outstanding payment could also be utilized to recover the aforesaid sum and interest.

6.1.5. 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.

6.1.6. 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.

6.1.7. To debar the BIDDER from participating in future bidding processes of the Bank for a minimum period of five years, which may be further extended at the discretion of the BUYER.

6.1.8. To recover all sums paid in violation of this Pact by Bidder(s) to any middleman or agent or broker with a view to securing the contract.

6.1.9. In cases where irrevocable letter of credit have been received in respect of any contract signed by the BUYER with the BIDDER, the same shall not be opened

6.1.10. Forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanctions for violation of this Pact.

7. Fail Clause:

7.1. The Bidder undertakes that it has not supplied / is not supplying similar products/systems or subsystems/ services 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 products/systems or sub systems was supplied by the Bidder to any other Ministry/Department of 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. The BUYER has appointed Independent Monitors (hereinafter referred to as Monitors) for this Pact in consultation with the Central Vigilance Commission (Names and Address of the Monitors to be given).

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 performs 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 Monitors 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 pocket documentation. The same is applicable to subcontractors. The Monitor shall be under contractual obligation to treat the information and documents of the BIDDER/subcontract(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/Secretary in the Department/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 correction problematic situations.

9. Facilitation of Investigation

In case of any allegation of violation of an 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 up to six 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 provisions 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 herby sign this Integrity Pact at ______________ on ________________

BUYER	BIDDER
Name of the Officer:	CHIEF EXECUTIVE OFFICER
Designation:	(Office Seal)

IT Department
Bank of Maharashtra
(Office Seal)
Place ____________________
Date ____________________

Witness:	Witness:
1 ___________________________	1 ___________________________
(Name & Address) : ____________	(Name & Address) : ____________
2 ___________________________	2 ___________________________
(Name & Address) : ____________	(Name & Address) : ____________

Annexure 14: Manufacturer’s Authorization Form

Note: This authorization letter should be printed on the letterhead of all the original equipment manufacturer (OEM) and should be signed by a competent person having the power of attorney to bind the manufacturer.

TO:

General Manager (IT),

Bank of Maharashtra Information Technology,

Head Office,

Lokmangal, Shivaji Nagar, Pune - 411005

Dear Sir,

Sub: RFP No: XX for supply, installation, commissioning and maintenance of security solutions (DLP, DICT, DAM, EE & PMS) dated: XX

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

We hereby extend our full guarantee and warranty 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 manufactured or distributed by the Bidder:

1. Such products as the Bank may opt to purchase from the Bidder, provided, that this option shall not relieve the Bidder of any warranty obligations under the contract; and
2. In the event of termination of production of such products:
    - Advance notification to the Bank of the pending termination, in sufficient time to permit the Bank to procure needed requirements; and
    - Following such termination, furnishing at no cost to the Bank, the blueprints, design documents, operations manuals, standards, source codes and specifications of the products, if requested.

We duly authorize the said firm to act on our behalf in fulfilling all installations, technical support and maintenance obligations required by the contract.

We further certify that, in case the authorized distributor/ system integrator is not able to meet its obligations as per contract during contract period, we, as the OEM, shall perform the said obligations with regard to their items through alternate & acceptable service provider.

Place:
Date:

Annexure 15: Resource Deployment Plan

Bidder should provide CV of the 2 proposed manpower for the tenure of the contract. Bidder also needs to fill the below resource deployment which it plans to deploy during the implementation phase of the project. This should comply with the minimum resource requirement mentioned in the RFP.

Resource name	Role	M 1	M 2	M 3	M 4	M 5	M 6	M 7	M 8	M 9	M 10	M 11	M 12
	Project Director												
	Enterprise Architect												
	PMO												

Note:

- F – Full Time
- P – Part Time Resource Deployment Plan during Support Phase

S. No.	Services	Resource Level (L1/L2/ L3)	Resou rce Type (Onsit e/ remote)	No of Resources Year 1	No of Resources Year 2	No of Resources Year 3	No of Resources Year 4	No of Resources Year 5
		Project Director						
		PMO						
		L3=1						
		L2=2 (DLP& DICT) L2=1 (DAM) L2=1 (PMS & EE)						
		L1=4 (Pooled Resources Operates 24x7x365)						

Note:

- Proposed Project Director is required to have implementation experience for solution in at least 2 Public Sector Bank/Scheduled Commercial Bank. Bidder is required to share CV of the proposed resources.
- Resource Deployment sheet shall be as per the support model proposed.
- Proposed model shall fulfil minimum requirements outlined in the RFP and as per the service window.
- Bidder should ensure that support model should meet SLA requirements and industry best practices.

Annexure 16: Guidelines, Terms & Conditions and Process Flow for E-Procurement Auction

Introduction:

Bank of Maharashtra intends to use E procurement Auction (Reverse Auction) process in place of submission of commercial bids of RFP NO **-** ______, dated ________

This annexure consists of rules for E Procurement Auction, Terms and conditions and Formats for submission of acceptance by the bidders.

1. Rules for E Procurement Auction (Reverse Auction):

a. **APPLICABILITY:**

i. Reverse Auctions are carried out under the framework of rules that are called Rules for Reverse Auction.

ii. All bidders participating in Reverse Auction shall understand/ accept and give an undertaking for compliance with the same to the Bank in the prescribed format as specified in **Annexure - 11**.

iii. Any bidder not willing to submit such an undertaking shall be disqualified for further participation respecting the procurement in question.

b. **ELIGIBILITY:**

i. Only bidders who are technically qualified and who submit the prescribed undertaking to the Bank alone can participate in Reverse Auction relevant to the procurement for which RFP is floated.

c. **COMPLIANCE/ CONFIRMATION FROM BIDDERS:**

i. The bidders participating in Reverse Auction shall submit the following duly signed by the Competent Authority who signs the offer documents in response to the RFP:

1. Acceptance of Rules for Reverse Auction and undertaking as per format in **Annexure-11**.
2. Agreement between service provider and bidder. (This format will be given by the service provider prior to announcement of Reverse Auction.)
3. Letter of authority authorizing the name/s of official/s to take part in Reverse Auction.

d. **TRAINING:**

i. The Bank will facilitate training for participation in Reverse Auction through the service provider for the Reverse Auction. During the training the Bidders shall be explained the rules related to the Reverse Auction to be adopted. Bidders are required to give compliance on it before the start of bid process.

ii. Wherever necessary, the Bank / service provider may also conduct a 'mock reverse auction' to familiarize the bidders with Reverse Auction process.

iii. Any bidder/bidder not participating in training and/or 'mock reverse auction' shall do so at his own risk and it shall not be open for him to make any complaint/grievance later.

iv. Each bidder / bidder shall participate in the training at his / their own cost.

e. **DATE/ TIME FOR TRAINING:**

i. The Venue, Date, Time etc. for training in Reverse Auction shall be informed later.

ii. No request for postponement/fixing of Training Date/Time shall be entertained which in the sole view and discretion of the Bank might result in any avoidable delay to either the Reverse Auction or the whole process of selection of bidder.

f. **DATE/ TIME OF REVERSE AUCTION:**

i. The Date and Time of commencement of Reverse Auction as also Duration of 'Reverse Auction Time' shall be communicated at least 7 working Days prior to such auction Date.

ii. Any force Majeure or other condition leading to postponement of auction shall entitle the Bank to postponement of auction even after communication, but, the Bank shall be obliged to communicate to all participating bidders the 'postponement' prior to commencement of such 'Reverse Auction'.

iii. Bank would not be liable for any failure of system, power failure, loss of internet connectivity, Inability to use the System, loss of electronic information, UPS failure etc.

g. **CONDUCT OF REVERSE AUCTION:**

i. The Reverse Auction shall be conducted on a specific web portal meant for this purpose.

ii. The Reverse Auction may be conducted by the Bank itself or through a service provider specifically identified/ appointed/ empaneled by the Bank.

h. **TRANSPARENCY IN BIDS:**

i. All bidders will be able to view during the auction time the current lowest price in portal. Bidder shall be able to view not only the lowest bid but also the last bid made by him at any point of time during the auction time.

i. **MASKING OF NAMES:**

  i. Names of bidders shall be masked in the Reverse Auction process and bidders will be given dummy names.

j. **START PRICE:**

  i. Bidders will fill the unit cost of the line items mentioned in **ANNEXURE-10 OF RFP** before the start of the bidding time as mentioned in clause no. f of this document. Once the bidding time starts the system will show the TCO of **ANNEXURE-10 OF RFP**. This total value is taken as the start price of the bidding process.

k. **DECREMENTAL BID VALUE**

  i. The bidders shall be able to bid only at a specified decrement value and not at any other fractions. The Bid decrement value shall be Rs.50,000/-.

  ii. The bid decrement value shall be in multiples of Rs. 50,000/-.

  iii. The web portal shall display the next possible decremented value of bid. It is not, however, obligatory on the part of bidders to bid at the next immediate lower level only. (That is, bids can be even at 2 or 3 lower levels than the immediate lower level).

  iv. Decremented value will be appropriated across the line items of **ANNEXURE-10** of RFP proportionately by the system.

l. **REVERSE AUCTION PROCESS:**

  i. The procurement process shall be completed through a single Reverse Auction.

  ii. The Bank shall however, be entitled to cancel the procurement of Reverse Auction process, if in its view procurement or reverse auction process cannot be conducted in a fair manner and / or in the interest of the Bank.

  iii. The bidder shall submit a confirmation of acceptance of the last bid price of auction within 30 minutes of closing of the auction to Bank either through Fax or E-Mail. The bidder has to submit the final bill of material as per **ANNEXURE-10 OF RFP** duly signed by the authorized official to Bank within 2 hours of close of auction by mail / fax.

  iv. In the event of circumstances like no power supply, system problem, loss of internet connectivity, inability to use the system, loss of electronic information, power interruptions, UPS failure, etc., the bidder has to ensure that they are able to convey their bidding price to the service provider by way of FAX, who will upload the Faxed price online on behalf of the bidder and confirm the receipt of FAX to the service provider. This should be done before the closure of bid time. The bidder has to ensure that the sufficient time is given to the Service provider to upload the faxed prices online. In case the required time is not available with the Service provider at the time of receipt of fax message, the Service provider will not be uploading the prices. It is thus requested from the bidders not to wait till the last moment to quote their bids so as to avoid any such complex situation.

m. **EXPENDITURE ON REVERSE AUCTION:**

i. All eligible bidders are requested to ensure that they have a valid digital certificate well in advance to participate in the Reverse auction process. The cost of digital certificate has to be borne by the bidder only.

ii. Bidders shall participate in the training or mock auction at their own cost.

n. **CHANGES IN BUSINESS RULES:**

i. Any changes made in Rules for Reverse Auction shall be informed to the eligible bidders before commencement of Reverse Auction.

o. **OTHER INSTRUCTIONS:**

i. No bidder shall involve himself / itself or any of his / its representatives in any price manipulation directly or indirectly with other bidders. If any such practice comes to the notice, Bank shall disqualify the bidder / bidders concerned from the reverse auction process.

ii. Bidder shall not disclose details of his bids or any other details concerning Reverse Auction process of the Bank to any other third party without specific permission in writing from the Bank.

iii. Neither Bank nor service provider can be held responsible for consequential damages such as no power supply, system problem, inability to use the system, loss of electronic information, power interruptions, UPS failure, etc.

p. **ERRORS AND OMISSIONS:**

i. On any issue or area of material concern respecting Reverse Auction not specifically dealt with in these Business Rules, the decision of the Bank shall be final and binding on all concerned.

Terms and conditions of Reverse Auction:

a. Each bidder will get a unique User Id and Password and bidders are requested to change the Password after the receipt of initial Password from the service provider. All bids made from the User ID given to the bidder will be deemed to have been made by the bidder. The auction type is English Reverse No Ties.

b. The duration of Auction will be of 30 minutes. If some bidder is bidding during the last 3 minutes of Auction closing, the Auction time will get extended for another 3 minutes from the time of the last accepted bid. Such extension will be allowed to continue till no bid is placed within 3 minutes of the last quote of such extended time. There is no restriction of extensions.

c. Auto-bid feature will be enabled from the start time of bidding. This feature will be explained during training to the bidders.

d. Bank of Maharashtra reserves the right to reject any or all the bids without assigning any reason whatsoever.

e. There shall be no variation between the on-line bid value and signed document to be submitted by the L1 bidder.

f. Bidding will be conducted in Indian Rupees (INR).

g. The bidder has to quote the total cost of items mentioned in **ANNEXURE-10 OF RFP** to arrive at the TCO.

h. The TCO amount after closure of reverse auction is final and shall be accepted by the L1 bidder.

i. The bids (Commercials) shall be firm for a period as specified in RFP and shall not be subjected to any change whatsoever.

j. Bidder has to submit acceptance to the terms and conditions of Reverse Auction and required compliance and other formats as mentioned in this document along with technical bids.

k. Bidder is not required to submit commercial bids in hard copy in a separate cover as mentioned in **RFP - XXXXX**, as Bank has decided to adopt Reverse Auction process for finalization of the bidder for placing the order.

l. Only those bidders who are technically qualified and competent to provide the required solution as per **RFP - XXXXXX** are only eligible to participate in Reverse Auction Process.

m. All eligible bidders are requested to ensure that they have a valid digital certificate well in advance to participate in the Reverse auction process.

Annexure 17: Past Experience

RFP NO: XX Dated: XX

Sr. No.	Customer Name	Brief scope of work (specify size of the client, implementation scope -modules and version, application support scope - number of years, date of go live etc.)	Attach reference Letter	Project Status (Live/ Under implementation)

(Enclose necessary documentary proof)

Annexure 18: List of Reports

Below list of reports is indicative and non-exhaustive. However, Bank and the successful bidder will prepare an exhaustive list of reports to be provided as a part of this solution.

- Device-based reports
- Software-based reports
- Policy-based reports
- User reports

Annexure 19: Performance Bank Guarantee

(ON A NON-JUDICIAL STAMP PAPER OF RS.500.00)

To,
Bank of Maharashtra,
I.T. Department, Head Office,
1501, Lokmangal,
Shivajinagar,
Pune - 411 005

Bank Guarantee No. : ___________
Amount of Guarantee : Rs. _______/-
Guarantee Valid up to: __ Months
Last date of lodgment of claim: ______20__

This deed of guarantee is executed on this ________Day of _________20__ by {Name of the Bank issuing guarantee} a body corporate, constituted under the Banking Companies (Acquisition and Transfer of Undertakings) Act 1970, having its Head office at (H.O. Address) and one of the Branch offices at (Branch address) (hereinafter referred to as the '**Guarantor Bank**', which expression unless it be repugnant to the context or meaning thereof shall include its successors and assigns) in favour of **Bank of Maharashtra**, a New Bank constituted by the Banking Companies (Acquisition and Transfer of Undertaking) Act 1970, and having its Head Office at Lokmangal, 1501, Shivajinagar, Pune-411005 (hereinafter referred to as **"Beneficiary Bank"**, which expression shall unless it be repugnant to the context or meaning thereof shall include its successors and assigns), for an amount not exceeding Rs. _______/- (Rs. _________________ only) at the request of M/s _____________________(with address).

Whereas engagement letter no. __________PO/LOI________ dated _________20__ (hereinafter called the **"Contract"**) for Rs.________/- (Rs. _________________________only) placed by the Beneficiary Bank on M/s ____________________, having its Head Office at ________________________and a branch office at ________________________________hereinafter referred to as **'Contractor'**) stands accepted by the contractor, and in terms of the said contract the contractor have to ____(Name of the Project)_____ as per the engagement letter referred hereinabove.

And whereas to ensure due performance to the satisfaction of the beneficiary Bank, of the services provided under the said contract and in terms thereof by the contractor as aforesaid, the Guarantor Bank at the request of the contractor has agreed to give guarantee as hereinafter provided.

NOW THIS GUARANTEE WITNESSETH AS FOLLOWS:-

In consideration of Bank of Maharashtra, the beneficiary bank, having issued engagement letter No. __________PO/LOI________ dated _________20__ for Rs.________/- (Rs. _________________________only) on M/s ____________________, having its Head Office at ________________________for ____(Name of the Project)_____ as per the engagement letter referred hereinabove, we, <Issuing Bank Name> do hereby undertake as under:

a) To indemnify and keep indemnified the beneficiary bank for the losses and damages that may be caused to or suffered by the beneficiary bank in the event of non-performance of whatever nature on the part of the contractor in discharging their contractual obligations under the said contract by the contractor against the above referred engagement letter and undertake this guarantee not exceeding Rs. ______/- (Rs. ________________________ only) without demur and without Beneficiary Bank needing to prove or to assign reasons for the demand so made for the sum specified therein and mere written claim or demand of the Beneficiary Bank shall be conclusive and binging on the guarantor Bank as to the amount specified under these presents.

b) The guarantee herein contained shall remain in full force and effect till discharged by the beneficiary bank or up to _____ months______, which is earlier.

c) This guarantee shall not in any way be affected by the change in the constitution of the contractor or of guarantor bank nor shall be affected by the change in the constitution, amalgamation, absorption or reconstruction of the beneficiary bank or otherwise but shall ensure for and be available to and enforceable by the absorbing amalgamated or reconstructed Company of the beneficiary bank.

d) To pay to the beneficiary Bank any money so demanded notwithstanding any dispute or disputes raised by the contractor in any suit or proceeding before any Court or Tribunal relating thereto our liability under this present being absolute and unequivocal.

e) We, ______________________________________ (indicate the name of Guarantor Bank with address) lastly undertake not to revoke this guarantee during its currency except with the previous consent of the Beneficiary Bank in writing, and the guarantee shall remain in full force and continuing till all dues claimed are paid

"Notwithstanding anything contrary contained in any law for the time in force or banking practice, this guarantee shall not be assignable or transferable by the beneficiary. Notice or invocation by any person such as assignee, transferee or agent of beneficiary shall not be entertained by the Bank. Any invocation of guarantee can be made only by the beneficiary directly."

Notwithstanding anything contained herein:

a) The Bank's liability …………………. not exceed Rs. ………….. (Rupees…………………………….)
b) This Bank Guarantee shall be valid up to …….………………… and
c) The Bank …………………….. on or before …………….. (Date of Expiry of Guarantee)
d) Every Guarantee shall be issued (regardless of the guarantee period) with a minimum claim period of one year from the date of expiry on

top of the guarantee period so as to avail benefit of Exception 3of the Section 28 of the Indian Contract Act, 1872. In other words, The Bank issuing such guarantee will not be liable under such guarantee to the beneficiary after the expiry of the claim period of one year, regardless of period of limitation under the Limitation Act, 1963. Commission for the claim period also be charged to the customer.

Or

If a Bank Guarantee is issued with a claim period of less than one year on top of the guarantee period, then such guarantee will not have the benefit of Exception 3 of the Section 28 of the Indian Contract Act, 1872. In other words, The Bank issuing such guarantee could stand exposed to period of limitation under the Limitation Act, 1963, which period is 30 years when the Government is the guarantee beneficiary and 3 years when any other party is the guarantee beneficiary."

IN WITNESS WHEREOF the authorized signatories of the said (Guarantor Bank) have signed this deed for and on behalf of the guarantor on the date first hereinabove mentioned.

Place:

SEAL

Code No.

SIGNATURE

Annexure 20: Authorization Letter

Format for Bid Opening

(To be brought at the time of opening of Bids)

Date DD-MM-YYYY

To

General Manager

Information Technology Department

Bank

Address

SUB: Authorization Letter for attending the Bid Opening

REF: YOUR RFP NO: dated XX/XX/XXXX

Dear Sir,

This has reference to your above RFP for implementation of proposed security solution(DLP, DICT, DAM, EE & PMS) in your Bank. Mr./Miss/Mrs. ____ is hereby authorized to attend the bid opening of the above RFP No.: dated xx/xx/2020 on _____________ on behalf of our organization.

The specimen signature is attested below:

Name:

_________________________________ (Specimen Signature of Representative)

____

Signature of Authorizing Authority

Name of Authorizing Authority Designation:

Company Seal

Annexure 21 Non-Disclosure Agreement

(ON A NON-JUDICIAL STAMP PAPER OF RS. 500)

This Confidentiality cum Non-disclosure Agreement is entered into at ________________on this day________of__________2019, between ______________________________ a company within the meaning of Companies Act, 1956/the Companies Act, 2013 having its Registered Office

____ and **Bank of Maharashtra**, a Body Corporate constituted under the Banking Companies (Acquisition & Transfer of Undertakings) Act, 1970 having its **Head Office at 1501, ‘LOKMANGAL’, Shivajinagar, Pune – 411 005 (herein after referred to as 'BOM' or “Bank”).**

____________ and BOM would be having discussions and negotiations concerning the establishment during continuance of a business relationship between them as per Agreement dated__________ (hereinafter referred to as 'Agreement'). In the course of such discussions and negotiations, it is anticipated that either party may disclose or deliver to the other party certain of its trade secrets or confidential or proprietary information for the purpose of enabling the other party to evaluate the feasibility of such a business relationship. The parties have entered into this Agreement, in order to assure the confidentiality of such trade secrets and confidential and proprietary information in accordance with the terms of this Agreement. As used in this Agreement, the party disclosing Proprietary Information (as defined below) is referred to as the 'Disclosing Party' and will include its affiliates and subsidiaries, the party receiving such Proprietary Information is referred to as the 'Recipient', and will include its affiliates and subsidiaries.

Now this Agreement witnesseth:

1 Proprietary Information: As used in this Agreement, the term 'Proprietary Information' shall mean all trade secrets or confidential or Proprietary Information designated as such in writing by the Disclosing Party, whether by letter or by the use of an appropriate prominently placed Proprietary stamp or legend, prior to or at the time such trade secret or confidential or Proprietary Information is disclosed by the Disclosing Party to the Recipient. Notwithstanding the forgoing, information which is orally or visually disclosed to the recipient by the Disclosing Party or is disclosed in writing unaccompanied by a covering letter, proprietary stamp or legend, shall constitute proprietary information if the disclosing party, within 10 (ten) days after such disclosure, delivers to the Recipient a written document or documents describing such Proprietary Information and referencing the place and date of such oral, visual or written disclosure and the names of the employees or officers of the Recipient to whom such disclosure was made.

2 Confidentiality

a) Each party shall keep secret and treat in strictest confidence all confidential information it has received about the other party or its customers and will not use the confidential information otherwise than for the purpose of performing its obligations under this Agreement in accordance with its terms and so far as may be required for the proper exercise of the Parties' respective rights under this Agreement. Any information considered sensitive must be protected by the Bidder from unauthorized disclosure or access.

b) The term 'confidential information' shall include all written or oral information (including information received from third parties that the 'Disclosing Party' is obligated to treat as confidential) that is (i) clearly identified in writing at the time of disclosure as confidential and in case of oral or visual disclosure, or (ii) that a reasonable person at the time of disclosure reasonably would assume, under the circumstances, to be confidential.

Confidential information shall also include, without limitation, software programs, technical data, methodologies, know-how, processes, designs, new products, developmental work, marketing requirements, marketing plans, customer names, prospective customer names, customer information and business information of the 'Disclosing Party'.

3. Non-Disclosure of Proprietary Information: For the period during the Agreement or its renewal, the Recipient will:

   (a) Use such Proprietary Information only for the purpose for which it was disclosed and without prior written authorization of the Disclosing Party shall not use or exploit such Proprietary Information for its own benefit or the benefit of others.

   (b) Protect the Proprietary Information against disclosure to third parties in the same manner and with the reasonable degree of care, with which it protects its confidential information of similar importance: and

   (c) Limit disclosure of Proprietary Information received under this Agreement to persons within its organization and to those third party contractors performing tasks that would otherwise customarily or routinely be performed by its employees, who have a need to know such Proprietary Information in the course of performance of their duties and who are bound to protect the confidentiality of such Proprietary Information.

4. Limit on Obligations : The obligations of the Recipient specified in clause 3 above shall not apply and the Recipient shall have no further obligations, with respect to any Proprietary Information to the extent that such Proprietary Information:

   a) Is generally known to the public at the time of disclosure or becomes generally known without any wrongful act on the part of the Recipient,

   b) Is in the Recipient's possession at the time of disclosure otherwise than as a result of the Recipient's breach of a legal obligation;

   c) Becomes known to the Recipient through disclosure by any other source, other than the Disclosing Party, having the legal right to disclose such Proprietary Information.

   d) Is independently developed by the Recipient without reference to or reliance upon the Proprietary Information; or

   e) Is required to be disclosed by the Recipient to comply with applicable laws or governmental regulation, provided that the recipient provides prior written notice of such disclosure to the Disclosing Party and takes reasonable and lawful actions to avoid and/or minimize the extent of such disclosure.

5. Return of Documents: The Recipient shall, upon the request of the Disclosing Party, in writing, return to the Disclosing Party all drawings, documents and other tangible manifestations of Proprietary Information received by the Recipient pursuant to this Agreement (and all copies and reproductions thereof) within a reasonable period. Each party agrees that in the event it is not inclined to proceed further with the engagement, business discussions and negotiations, or in the event of termination of this Agreement, the Recipient party will promptly return to the other party or with the consent of the other party, destroy the Proprietary Information of the other party.

6. Communications: Written communications requesting or transferring Proprietary Information under this Agreement shall be addressed only to the respective designees as follows (or to such designees as the parties hereto may from time to time designate in writing)

MIS ____________________   *Bank of Maharashtra*

*Attn:*_____________________ *Attn:*__________________

7. Term: The obligation pursuant to Clause 2 and 3 (Confidentiality and Non-Disclosure of Proprietary Information) will survive forever following the term of the Agreement dated__________.
    a. Nothing herein contained shall be construed as a grant by implication, estoppels, or otherwise or a license by either party to the other to make, have made, use or sell any product using Proprietary Information or as a license under any patent, patent application, utility model, copyright or any other industrial or intellectual property right covering same.

8. Damages: The provisions of this Agreement are necessary for the protection of the business goodwill of the parties and are considered by the parties to be reasonable for such purposes. Both the parties agree that any breach of this Agreement will cause substantial and irreparable damages to the other party and, therefore, in the event of such breach, in addition to other remedies, which may be available, the party violating the terms of Agreement shall be liable for the entire loss and damages on account of such disclosure.
   Each party agrees to indemnify the other against loss suffered due to breach of contract and undertakes to make good the financial loss caused directly or indirectly by claims brought about by its customers or by third parties.

9. Miscellaneous:

   a) This Agreement may not be modified, changed or discharged, in whole or in part, except by a further Agreement in writing signed by both the parties.

   b) This Agreement will be binding upon and ensure to the benefit of the parties hereto and it also includes their respective successors and assignees

   c) The Agreement shall be construed and interpreted in accordance with the laws prevailing in India.

   In witness whereof, the parties hereto have agreed, accepted and acknowledged and signed these presents, on the day, month and year mentioned herein above.

For ________________________ Authorized Signatory

Shri ________________________ Designation _________________

For Bank of Maharashtra Authorized Signatory

Shri ________________________ Designation _________________

Annexure 22 Resource Plan Matrix

Role	Type	Activity	Experience		Qualification & Experience
			Total	Security Solutions	
Solution Administration & Management	L1	The L1 resources at this level shall be able to address the primary level diagnosis, monitoring of the functioning of the solution, address the user complaints and resolve the primary level calls over the phone / deskside, timely escalations to the next level support (L2) & follow up on the closure of the events. The L1 level support resource/s will be pool of resources across the deployed solutions of this RFP.	3+	2+	B.E./B.Tech./ M.E./M.Tech /BCA/B.Sc./ MCA/M.Sc. with a minimum relevant experience of two years in respective solution of RFP.
Solution Administration & Management	L2	The resources at this level shall be able to address the escalations of L1 support staff, monitoring, administration & management of the deployed solution. These resources will be the specialized resources of the respective product and must have exposure in Policy/Rule Creation/Fine-Tuning and Data Collection Tasks.	4+	3+	B.E./B.Tech./ M.E./M.Tech /BCA/B.Sc./ MCA/M.Sc. a minimum Three years' experience in the respective solution of RFP.
Solution Administration & Management	L3	The resources at this level shall be able to address the all escalations. The resources should have knowledge of Information Security Framework such as ISO27001, Risk Management Framework such as ISO31000, IT Service Management	5+	4+	B.E./B.Tech./ M.E./M.Tech /BCA/B.Sc./ MCA/M.Sc. with minimum Five years' experience on respective solution of RFP & should have expert level knowledge on related Network & Information security solutions.

Annexure 23 Undertaking of Information Security

(This letter should be on the letterhead of the bidder as well as the OEM/ Manufacturer duly signed by an authorized signatory on Information security as per regulatory requirement)

To,
The Deputy General Manager
Information Technology,
Bank of Maharashtra,
Lokmangal, 1501,
Shivajinagar, Pune

Sir,

Sub: RFP for Supply, Installation and Maintenance of security Solutions (DLP, DICT, DAM, EE & PMS).

We hereby undertake that the proposed software to be supplied to the Bank 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)

Yours faithfully,

Authorized Signatory

Name:
Designation:
Bidder’s Corporate Name Address
Email and Phone

Annexure 24 List of supported devices by OEM

Sr No	Vendor	Name of the device	Device type	Versions of devices supported	Knowledge base reference	remarks

Annexure 25 End of Sale/ End of Support/ End of Life Information

Sr no	Solution	Component Type	End of Sale	End of Support	End of Life
	Security Solution (DLP, DICT, DAM, EE & PMS)	Hardware (add rows if required)			
		Software (add rows if required)			
		License			
		Supporting hardware if any (such as NAS, Hardware agent etc)			
		Supporting software if any (such as OS etc)			
		Database			

***** Similar information is to be provided for all other proposed solutions.**

Annexure 26 Compliance Agreement

We communicate our unconditional acceptance to the following terms and conditions of RFP XXXXXX

1) We acknowledge that we have received, read, understood and agreed to all terms (including payment terms) in the Tender Document no. XXXXXX for the Supply, Installation & Maintenance of Security Solutions (Data Loss Prevention (DLP), Data Identification & Classification Tool (DICT), Database Activity Monitoring (DAM), Endpoint Encryption (EE) & Patch Management Solution (PMS)).
2) We agree that we cannot change Price or Quantity or Quality or Delivery terms or Technology & Service levels (or any other terms that impact the price) post the bid event without prior consent of Bank of Maharashtra.
3) We agree that we are deemed to have accepted the all rules on participation at the bid. Bank of Maharashtra will make every effort to make the bid process transparent. However, the award decision by Bank of Maharashtra would be final and binding on us.
4) We agree not to divulge either our bids or those of other suppliers to any other external party.
5) Bank of Maharashtra has implemented ISMS framework, hence we agree to abide by the required integrations of security policies of the Bank.
6) Proposed Security Solutions shall be kept in compliance to the various statutory requirements specified by RBI/Cert-In/NCIIPC from time to time in future
7) We agree to non-disclosure of trade information regarding the purchase, part specifications, and identity of Bank of Maharashtra, bid process, bid technology, bid documentation and bid details. Bank of Maharashtra tender documents remain the property of Bank of Maharashtra and all suppliers are required to return these documents to Bank of Maharashtra upon request.
8) Bank of Maharashtra’s decision will be final and binding on us and would be based on Strategic Sourcing Evaluation, Current Service Performance and Actual Compliance of Agreed Specifications.
9) Splitting of the award decision over a number of suppliers or parts or over time (as in the case of staggered deliveries) will be at Bank of Maharashtra’s discretion.
10) Bids once made cannot be withdrawn or modified under any circumstances. Only blatant typing errors would be withdrawn from bid. The decision of Bank of Maharashtra would be final and binding on all bidders.
11) Bank of Maharashtra has the right to decide to extend, reschedule, cancel the RFP.
12) Please note that Bank of Maharashtra may consider debarring a supplier in the event the supplier violates terms and conditions mentioned in this compliance agreement.
13) We have read the Bank of Maharashtra technical specifications & drawings for various products in detail & have agreed to comply with Quality, Technology & Service expectations.
14) Product specifications offered in technical bid will remain unchanged. No diversification / substitution of products will be entertained.
15) If successful, we are agreed to provide uninterrupted service for next 5 years.

We agree to have read and understood the Compliance Agreement in its entirety and agree to abide by this Statement.

Name: Stamp:
Designation: Place: Date:
Organization: Signature

END OF DOCUMENT